Tell us about your PDF experience.

Windows client troubleshooting

This library provides solutions enabling IT Pros to troubleshoot and support devices running Windows client operating systems in a server environment. To bring you the most accurate content, this library is managed by a team that works directly with the Windows product group and support professionals.

Deployment

HOW-TO GUIDE

Deployment

Windows 7 End of Support (EoS) FAQ

Identity and Access

HOW-TO GUIDE

Active Directory

Group Policy

UserProfiles and Logon

Networking

HOW-TO GUIDE

Networking

Storage and High Availability

HOW-TO GUIDE

Backup and Storage

High Availability

Virtualization

User Experience

HOW-TO GUIDE

Application Virtualization (App-V)

Application Management

Printing

Remote Desktop Services

System Management Components

UE-V

Windows Performance

HOW-TO GUIDE

Performance

Shell Experience

Windows Security

HOW-TO GUIDE

Windows Security

Management

HOW-TO GUIDE

Admin Development

Windows Troubleshooters

Windows Troubleshooters

Windows Troubleshooters

HOW-TO GUIDE

Active and retired troubleshooters for Windows 10

Active Directory troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Active Directory-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Active Directory sub categories

- Schema update - known issues, best practices, workflow review
- User, computer, group, and object management
- Windows Time Service

Error when you check domain object properties by using RSAT in Windows 10: msDS-ExpirePasswordsOnSmartCardOnlyAccounts not exist

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an error that occurs when you check domain object properties by using RSAT in Windows 10.

Applies to: Windows 10, version 1809
Original KB number: 3214525

Symptoms

You have a Windows 10, version 1809-based client that joins a domain with a Windows Server 2012 R2 controller. Additionally, the Remote Server Administration Tools (RSAT) for Windows 10 is installed on the client. When you right-click the properties of a domain object in Active Directory Administrative Center (ADAC) in this situation, you receive the following error message:

> Failed to retrieve the object 'DC=CONTOSO,DC=COM' due to the following error: The specified directory service attribute or value does not exist Parameter name: msDS-ExpirePasswordsOnSmartCardOnlyAccounts

Cause

This issue occurs when the schema version of the domain has not yet been updated.

Workaround

To work around this issue, use one of the following tools to obtain the properties of a domain object:

- DSA.msc
- Ldifde.exe
- Ldp.exe

- ADSI Edit (adsiedit.msc)
- Get-ADObject cmdlets

Known issues managing a Windows 10 Group Policy client in Windows Server 2012 R2

Article • 03/24/2022 • 19 minutes to read

Applies to: Window 10 - all editions, Windows Server 2019, Windows Server 2012 R2
Original KB number: 4015786

Summary

When you manage a Windows 10 Group policy client base from a Windows Server 2012 R2 server, some known challenges can occur. The same challenges apply to using the Advanced Group Policy Management server (AGPM) on a Windows Server 2012 R2 server when you manage Windows 10 clients.

This article is separated into sections for each subsequent upgrade as they were released. It also indicates when a change affects only a specific build of the Group Policy ADMX template files.

The following list of changes doesn't include the many new additional settings that are added to each template file. They don't have any effect if they're added to an existing deployment. The existing deployment doesn't use those settings. So, it's unlikely to affect the environment.

It's also important to consider that during the GPMC startup, the console caches the ADMX files into memory. Any changes to the templates that occur while the tool is open don't appear, even after a report refresh. After the tool is shut down and then reopened, it will get the new ADMX files from the PolicyDefinitions folder.

More information

Traditionally, the method of translating group policy settings into a user interface that could be easily managed was provided by ADM files. These files use their own markup language. They were locale-specific. So, they were difficult to manage for multinational companies.

Windows Vista and Windows Server 2008 introduced a new method of displaying settings within the Group Policy Management Console. Registry-based policy settings are defined as using a standards-based, XML file format known as ADMX, more commonly known as administrative templates. These settings are located under the Administrative Templates category in the Group Policy Object Editor.

Group Policy Object Editor and Group Policy Management Console remain largely unchanged. In most situations, you don't notice the presence of ADMX files during your daily Group Policy administration tasks.

In some situations, you need to understand:

- how ADMX files are structured
- the location where they're stored

ADMX files provide an XML-based structure. This structure is used for defining the display of the Administrative Template policy settings in the Group Policy tools. The Group Policy tools recognize ADMX files only if you're using a computer that is running Windows Vista or Windows Server 2008 or later versions.

Unlike ADM files, ADMX files aren't stored in individual GPOs. For domain-based enterprises, administrators can create a central store location of ADMX files. And this location is accessible by anyone who has permission to create or edit GPOs. Group Policy tools continue to recognize any custom ADM files in your existing environment. But they will ignore any ADM file that has been superseded by an ADMX file, such as:

- System.adm
- Inetres.adm
- Conf.adm
- Wmplayer.adm
- Wuau.adm

If you've edited any of these files to change or create policy settings, the changed or new settings aren't read or displayed by the Windows Vista-based Group Policy tools.

The Group Policy Object Editor automatically reads and displays Administrative Template policy settings from ADMX files that are stored locally or in the optional ADMX central store. The Group Policy Object Editor automatically reads and displays Administrative Template policy settings from custom ADM files that are stored in the GPO. You can still add or remove custom ADM files by using the Add/Remove template menu option. All Group Policy settings currently in ADM files that are delivered by Windows Server 2003, Windows XP, and Windows 2000 are also available in Windows Vista and Windows Server 2008 ADMX files.

It can be challenging to upgrade the PolicyDefinitions folder that has later revisions of the ADMX files. The reason is that some settings are deprecated and some are added. Typically, adding settings has a minimal effect. However, deprecating settings often causes pre-configured Group Policies to keep settings that can no longer be changed. Commonly, those types of redundant settings from the new ADMX files are listed as Extra Registry Settings in the settings report. These settings are still applied to production, but the administrator can no longer turn them on or off.

To manage this situation, an administrator could delete the Group policy, if it's no longer required. Or, they could copy the legacy ADMX template back to the PolicyDefinitions folder. It would enable the setting to be managed again. But the new settings from the later revision ADMX template are lost.

Known ADMX file content change issues in Windows 10 build 1607

Filename	Change	Possible effect
DataCollection.admx	Changed Policy setting `Allow Telemetry` class value from **Machine** to **Both**	This ADMX first appeared in Windows 10 RTM and was set to Machine in both the RTM and 1511 revisions. In build 1607, the class changed to **Both**. It means that the setting was applicable to both the User and Machine sides of the registry. Because it's an extension of an existing setting, this change has no expected effect.
DeliveryOptimization.admx	Changed Policy setting **Download Mode** (DownloadMode) configuration item from **None** to **HTTP only**	This change is a display text change only. The underlying values are the same as for previous builds of the ADMX file. So, there's no effect on production group policies.
inetres.admx	Removed Policy setting **Show Content Advisor on Internet Options**	This setting was deprecated from the 1607 build of the ADMX file, which has been present pre-2012 and Windows 8. The setting remains configured under the following conditions: • the setting had already been deployed into production • the ADMX file was upgraded But it can't be changed without using one of the following methods: • using a custom ADMX • deleting the whole policy that stores the setting.

Filename	Change	Possible effect
MicrosoftEdge.admx	The following 15 settings have had class changes from **Machine** to **Both**: • Configure Autofill (AllowAutofill) • Allow Developer Tools (AllowDeveloperTools) • Configure don't Track (AllowDoNotTrack) • Allow InPrivate browsing (AllowInPrivate) • Configure Password Manager (AllowPasswordManager) • Configure Pop-up Blocker (AllowPopups) • Configure SmartScreen Filter (AllowSmartScreen) • Allow web content on New Tab page (AllowWebContentOnNewTabPage) • Configure cookies (Cookies) • Configure the Enterprise Mode Site List (EnterpriseModeSiteList) • Prevent using Localhost IP address for WebRTC (HideLocalHostIPAddress) • Configure Home pages (HomePages) • Prevent bypassing SmartScreen prompts for files (PreventSmartScreenPromptOverrideForFiles) • Configure Favorites (Favorites) • Send all intranet sites to Internet Explorer 11 (SendIntranetTraffictoInternetExplorer)	This ADMX first appeared in Windows 10 RTM, and was set to **Machine** in both the RTM and 1511 revisions. In build 1607, the class changed to Both. It means that the setting was applicable to both the User and Machine sides of the registry. Because it's an extension of an existing setting, this change has no expected effect.
WindowsDefender.admx	Removed Policy setting **Define the rate of detection events for logging**	This setting was deprecated from the ADMX file. The setting remains configured under the following conditions: • the setting had already been deployed into production • the ADMX file was upgraded But it can't be changed without using one of the following methods: • using a custom ADMX • deleting the whole policy that stores the setting.
WindowsDefender.admx	Removed Policy settings **IP address range Exclusions** and **Port number Exclusions**	This setting was deprecated from the ADMX file. The setting remains configured under the following conditions: • the setting had already been deployed into production • the ADMX file was upgraded But it can't be changed without using one of the following methods: • using a custom ADMX • deleting the whole policy that stores the setting.
WindowsDefender.admx	Removed Policy setting **Process Exclusions for outbound traffic**	This setting was deprecated from the ADMX file. The setting remains configured under the following conditions: • the setting had already been deployed into production • the ADMX file was upgraded But it can't be changed without using one of the following methods: • using a custom ADMX • deleting the whole policy that stores the setting.

Filename	Change	Possible effect
WindowsDefender.admx	Removed Policy setting **Threat ID Exclusions**	This setting was deprecated from the ADMX file. The setting remains configured under the following conditions: • the setting had already been deployed into production • the ADMX file was upgraded But it can't be changed without using one of the following methods: • using a custom ADMX • deleting the whole policy that stores the setting.
WindowsDefender.admx:	Removed Policy setting **Turn on Information Protection Control**	This setting was deprecated from the ADMX file. The setting remains configured under the following conditions: • the setting had already been deployed into production • the ADMX file was upgraded But it can't be changed without using one of the following methods: • using a custom ADMX • deleting the whole policy that stores the setting.
WindowsDefender.admx	Removed Policy setting **Turn on network protection against exploits of known vulnerabilities**	This setting was deprecated from the ADMX file. The setting remains configured under the following conditions: • the setting had already been deployed into production • the ADMX file was upgraded But it can't be changed without using one of the following methods: • using a custom ADMX • deleting the whole policy that stores the setting.
WindowsDefender.admx	Changed Policy setting **Suppress all notifications** (UX_Configuration_Notification_Suppress) enabled and disabled value from enabledValue=0 and disabledValue=1 to enabledValue=1 and disabledValue=0	This change has occurred on build 1607 and differs from build 1511 and previous. The change enables this setting to work as expected, because to previously enable this setting, it had to be disabled. The impact for an upgrade is: if the setting was configured and the PolicyDefinitions were upgraded to 1607, then the setting would automatically revert to the opposite setting that was previously configured. See Appendix 1 Windows Defender
WindowsDefender.admx	Removed Policy setting **Configure local setting override to turn off Intrusion Prevention System**	This setting was deprecated from the ADMX file. The setting remains configured under the following conditions: • the setting had already been deployed into production • the ADMX file was upgraded But it can't be changed without using one of the following methods: • using a custom ADMX • deleting the whole policy that stores the setting.
WindowsExplorer.admx	Changed Policy setting **Configure Windows SmartScreen** (EnableSmartScreen), replaced drop-down item to enabled/disabled configuration item.	This setting has changed in this version from previous versions, in particular the option to enable smart screen but Require approval from an administrator before running downloaded unknown software has been deprecated. If this setting was configured previously, it will become unmanageable after the ADMX upgrade. If this setting is enabled, but the smart screen was disabled, then the whole setting becomes disabled after the upgrade. See Appendix 2 Windows Explorer

Filename	Change	Possible effect
WindowsUpdate.admx	Removed Policy setting **Defer Upgrades and Updates** (DeferUpgrade), replaced by more detailed Policy settings (`DeferFeatureUpdates`, `DeferQualityUpdates`, `ExcludeWUDriversInQualityUpdate`, `ActiveHours`)	The defer upgrade option was made available as per Windows 10 RTM and was changed on build 1607. Once the settings have been configured, and the `PolicyDefinitions` folder is upgraded to build 1607, the settings become unmanageable. The configured settings will remain configured. But it can't be changed without using one of the following methods: • using a custom ADMX • deleting the whole policy that stores the setting. As the new DeferUpgrade settings are new to build 1607, it isn't expected to affect existing configurations. See Appendix 3 Windows Update

Known ADMX file content change issues in Windows 10 build 1511

Filename	Change	Possible Effect
Explorer.admx	Removed Policy setting **Turn off soft landing help tips** (DisableSoftLanding)	This setting has been deprecated from the Window 10 RTM ADMX file and wasn't present in 2012 R2. If the setting had already been deployed into production and the ADMX was upgraded, the setting remains configured. But it can't be changed without using one of the following methods: • using a custom ADMX • deleting the whole policy that stores the setting.
inetres.admx	Removed Policy setting **Prevent configuration of top-result search on Address bar** (TopResultPol) (computer/Windows Components/IE/Internet Settings/Advanced Settings/Searching)	This setting has been deprecated from the ADMX file. If the setting had already been deployed into production and the ADMX was upgraded, the setting remains configured. But it isn't changeable without either using a custom ADMX or deleting the whole policy that stores the setting.
LocationProviderAdm.admx	Deprecated Microsoft-Windows-Geolocation-WLPAdm.admx for the new filename LocationProviderAdm.admx	When you upgrade from Windows 10 RTM to Windows 10 version 1511, the new LocationProviderAdm.admx file is copied to the folder while keeping the old Microsoft-Windows-Geolocation-WLPAdm.admx file. So, there are two ADMX files that address the same policy namespace. This generating an error. See "'Microsoft.Policies.Sensors.WindowsLocationProvider' is already defined" error when you edit a policy in Windows
MicrosoftEdge.admx	Removed Policy setting **Allows you to run scripts, like JavaScript** (AllowActiveScripting) (Computer)	This setting has been deprecated from the ADMX file. If the setting had already been deployed into production, and the ADMX was upgraded, the setting remains configured. But it won't be changeable without either using a custom ADMX or deleting the whole policy that stores the setting.
MicrosoftEdge.admx	The following nine settings have had class changes from **Both** to **Machine**: • Turn off Autofill (AllowAutofill) Allow employees to send don't Track headers (AllowDoNotTrack)Turn off Password Manager (AllowPasswordManager)Turn off Pop-up Blocker (AllowPopups)Turn off address bar search suggestions (AllowSearchSuggestionsinAddressBar)Turn off the SmartScreen Filter (AllowSmartScreen)Configure Cookies (Cookies)Configure the Enterprise Mode Site List (EnterpriseModeSiteList)Send all intranet sites to Internet Explorer 11 (SendIntranetTraffictoInternetExplorer)	Change from **Both** to **Machine** means: a setting is descoped from being applicable to both the User and Machine sides of a policy to only the Machine side. If the policy has already been configured in the User side, you can't change the user side settings again after the ADMX upgrade. However, the setting remains configured.

Filename	Change	Possible Effect
ParentalControls.admx	Was removed in this build of ADMX	When an ADMX is removed from the latest build of templates, all settings that may have been configured from previous versions of the file become stagnant. If the `PolicyDefinitions` folder is upgraded, the existing previous file is still present. So, there's no effect. The settings will still be present and functional if the following conditions are true: • the content of the `PolicyDefinitions` folder is removed • the new templates are populated • some group policies are still configured by using the settings from parentalcontrols.ADMX However, they can't be reconfigured without either using a custom ADMX or deleting the whole policy that stores the setting.
WindowsStore.admx	Was added, that directly replaces WinStoreUI.admx (obtained from Windows 2012/8 RTM ADMX and wasn't present in 2012 R2/8.1)	The **EnableWindowsStoreOnWTG** setting in the key named `Software\Policies\Microsoft\WindowsStore` that has the value name of **EnableWindowsStoreOnWTG** is deprecated. It prevents the setting from being reconfigurable without either using a custom ADMX or deleting the whole policy that stores the setting. Also, the DisableAutoDownload setting value is changed from 3 (winStoreUI) to 4 (WindowsStore). It causes the original setting to be superseded and appear under extra registry settings. It also causes the original setting to become unchangeable. However, it will still be set. See Appendix 4 WinStoreUI upgrade to WindowsStore. If both files are present at the same time, the GPMC fails to load. It's because the namespaces of both files are also duplicates. It causes the error while generating the settings `reportNamespace` 'Microsoft.Policies.WindowsStore' is already defined as the target namespace for another file in the store. File \\<Domain Name>\SysVol<DomainName>\Policies\PolicyDefinitions\WinStoreUI.admx, line 4, column 80

Known ADMX file content change issues in Windows 10 RTM

Filename	Change	Possible effect
AppXRuntime.admx	Changed Policy **Allow Microsoft accounts to be optional** class value change from **Both** to **Machine**	It means that a setting has been descoped from being applicable to both the User and Machine sides of a policy to just the Machine. If the policy has already been configured in the User side, you can't change the User side settings again after the ADMX upgrade. However, the setting remains configured.
ErrorReporting.admx	Removed Policy setting **Automatically send memory dumps for OS-generated error reports** (WerAutoApproveOSDumps_1 (User setting), WerAutoApproveOSDumps_2 (Machine setting))	If the ADMX is upgraded in place from the Windows Server 2012 R2 version, you can't change the settings again. The setting remains configured. However, you can't change it without either using a custom ADMX or deleting the whole policy that stores the setting.
ErrorReporting.admx	Removed Policy setting **Configure Default consent** (WerDefaultConsent_1 (User setting), WerDefaultConsent_2 (Machine setting))	Once the ErrorReporting.ADMX is replaced from the 2012 R2 revision to the Windows 10 RTM version, you see the following error: **Registry value DefaultConsent is of unexpected type.** To resolve this issue, remove the Group Policy, and rebuild the settings into a new policy using the new ADMX template. See Appendix 5 Error reporting
inetres.admx	Removed Policy setting **Allow Internet Explorer to use the SPDY/3 network protocol**	This setting has been deprecated from the 2012 R2 ADMX file. If the setting had already been deployed into production and the ADMX was upgraded, the setting remains configured. However, you can't change it without either using a custom ADMX or deleting the whole policy that stores the setting.

Filename	Change	Possible effect
NAPXPQec.admx	The ADMX file has been deprecated.	When an ADMX has been removed from the RTM build of templates, all settings that may have been configured from previous versions of the file become stagnant. If the PolicyDefinitions folder has been upgraded, the existing previous file remains present. So, there's no effect. The settings remain present and functional if the following conditions are true: • the content of the PolicyDefinitions folder has been removed • the new templates are populated • there are group policies still configured by using the settings from the NAPXPQec.ADMX But you can't reconfigure them without using one of the following methods: • using a custom ADMX • reinserting the file from a backup • deleting the whole policy that stores the setting.
NetworkProjection.admx	The ADMX file has been deprecated.	When an ADMX has been removed from the RTM build of templates, all settings that may have been configured from previous versions of the file becomes stagnant. If the PolicyDefinitions folder has been upgraded, then the existing previous file will still be present, so there will be no effect. The settings remain present and functional if the following conditions are true: • the content of the PolicyDefinitions folder is removed • the new templates are populated • there are group policies still configured by using the settings from the NetworkProjection.ADMX But you can't reconfigure them without using one of the following methods: • using a custom ADMX • reinserting the file from a backup • deleting the whole policy that stores the setting.
PswdSync.admx	This file was removed and now only delivered with Server Operating Systems only	When an ADMX has been removed from the RTM build of templates, all settings that may have been configured from previous versions of the file will become stagnant. If the PolicyDefinitions folder has been upgraded, the existing previous file will remain present, so there will be no effect. The settings remain present and functional if the following conditions are true: • the content of the PolicyDefinitions folder has been removed • the new templates are populated • there are group policies still configured by using the settings from the PswdSync.ADMX But you can't reconfigure them without using one of the following methods: • using a custom ADMX • reinserting the file from a backup • reinserting the file from a server build • deleting the whole policy that stores the setting.

Filename	Change	Possible effect
SkyDrive.admx	There are many changes to this file from 2012 R2 revision, but all change references from Skydrive to OneDrive, with relevant registry location changes also. Below are a few examples: 1. Changed policyNamespace from "target prefix="skydrive" namespace="Microsoft.Policies.Skydrive"" to "target prefix="onedrive" namespace="Microsoft.Policies.OneDrive"" 2. Changed category Skydrive to OneDrive 3. Changed policy **Prevent the usage of OneDrive for file storage** to use the OneDrive registry key (`Software\Policies\Microsoft\Windows\OneDrive`) from the Skydrive registry key (`Software\Policies\Microsoft\Windows\Skydrive`)	After the Windows 10 RTM version of the Skydrive.admx replaces the 2012 R2 revision of the file, all control of Skydrive components is replaced with the OneDrive versions settings. If you're still using the Skydrive application, those settings will still apply. However, they'll be unmanageable without either using a custom ADMX or recovering the 2012 R2 version of the template.
Snis.admx	This file was removed and now only delivered with Server Operating Systems only	When an ADMX has been removed from the RTM build of templates, all settings that may have been configured from previous versions of the file will become stagnant. If the PolicyDefinitions folder has been upgraded, the existing previous file will remain present. So, there's no effect. The settings remain present and functional if the following conditions are true: • the content of the PolicyDefinitions folder is removed • the new templates are populated • there are group policies still configured by using the settings from the Snis.ADMX However, you can't reconfigure them without using one of the following methods: • using a custom ADMX • reinserting the file from a backup • deleting the whole policy that stores the setting.
TerminalServer.admx	Changed Policy setting **Optimize visual experience when using RemoteFX** (TS_RemoteDesktopVirtualGraphics), removed typing error from **...ScreeenImageQuality...** to **...ScreenImageQuality...**	This setting has been changed internally and its name reference is only used to link the ADMX file to the ADML content. This change has no impact to the actual settings configured or the use of the settings in the policy.
WinStoreUI.admx	The ADMX file has been deprecated.	This file was removed from Windows 10 RTM. If the Microsoft Store was configured using Windows Server 2012 R2, these settings will become extra registry settings. The settings are still present and functional. But you can't reconfigure them without either using a custom ADMX or deleting the whole policy that stores the setting. Note: This file was replaced in Windows 10 build 1511 with the file WindowsStore.ADMX. Read the details of that file in the next section.

ADMX source file references

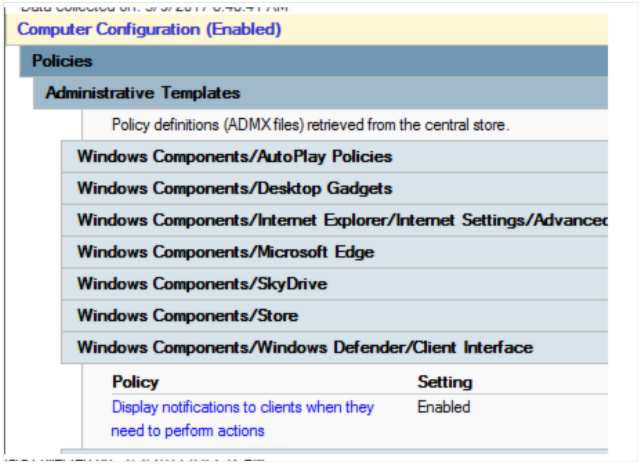
Filename	Reference Build	Revision Number	Digital Signal Date
Windows8-Server2012ADMX-RTM.msi	RTM	{EEDEB0DE-8C60-4EB6-A04D-7B3C5E121D03}	Thursday, January 24, 2013 10:08:25 PM
Windows8.1-Server2012R2ADMX-RTM.msi	RTM	{4AED4C7A-9B51-445C-9066-91F3CEE0E690}	Monday, November 25, 2013 2:09:46 AM
Windows10-ADMX.msi	RTM	{79A07922-2B64-445E-B6DD-5578B607A411}	Monday, August 3, 2015 6:07:15 AM
Windows10_Version_1511_ADMX.msi	1511	{095735F1-0D68-4941-A4CE-16BDEC8CAF21}	Tuesday, November 17, 2015 7:38:18 AM
Windows 10 and Windows Server 2016 ADMX.msi	1607	{7848F166-A24F-4AE3-AEC9-6622770F8A85}	Monday December 19, 2016 2:07:42 PM,

Other references

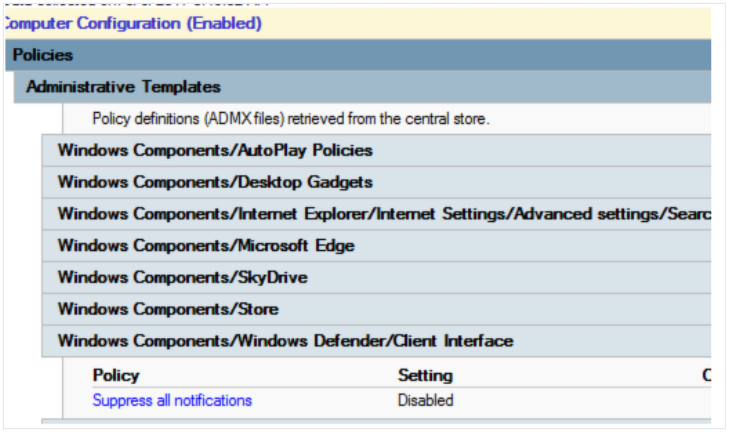
- How to create and manage the Central Store for Group Policy Administrative Templates in Windows
- Managing Group Policy ADMX Files Step-by-Step Guide
- "'Microsoft.Policies.Sensors.WindowsLocationProvider' is already defined" error when you edit a policy in Windows
- ADMX Version History
- The content differences between ADMX/L files, within an Excel spreadsheet are available here: https://go.microsoft.com/fwlink/?linkid=829685.

Appendix

Appendix 1 Windows Defender

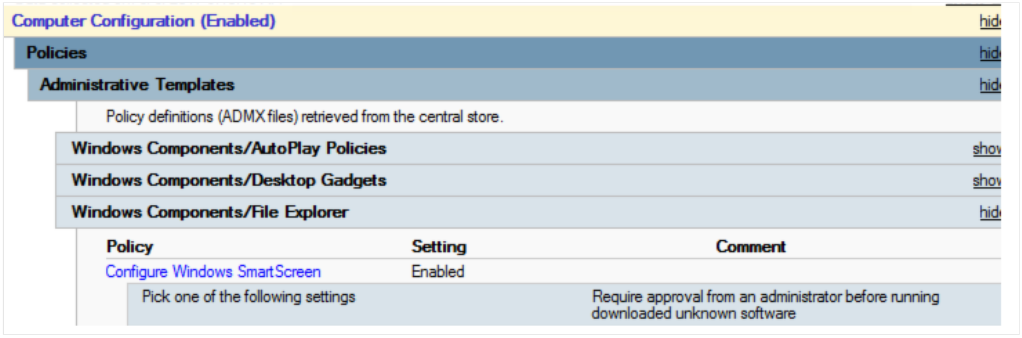


The same setting (without editing the policy) after an ADMX upgrade to 1607d

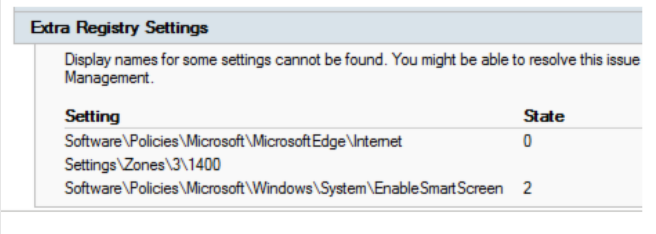


Appendix 2 Windows Explorer

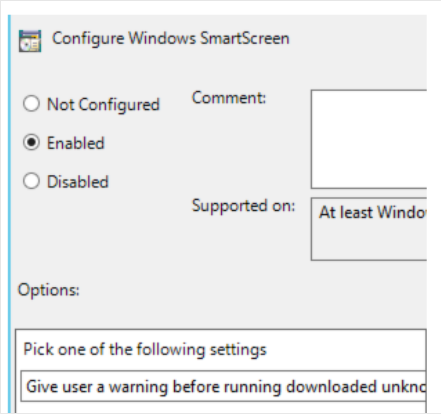
If the SmartScreen setting is enabled, and the **Require approval from an administrator before running downloaded unknown software** option is selected, you see:



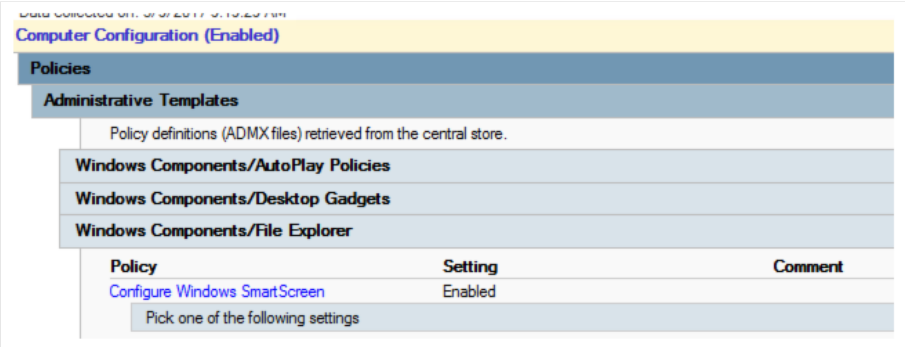
After you upgrade the templates directly without changing the policy, you see:



If you select the second option ("Give a warning"), you see:

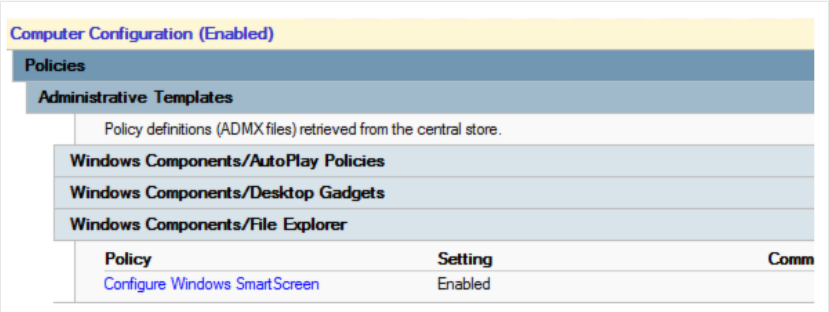


However, in the settings tab of GPMC, you see:

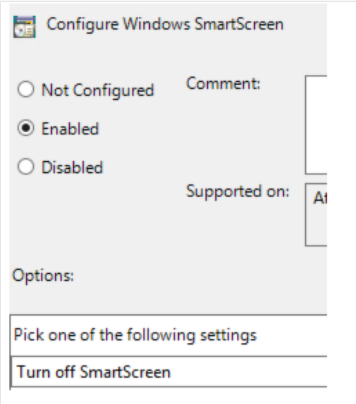


> ⓘ Note
>
> No items are listed under **Pick one of the following settings**.

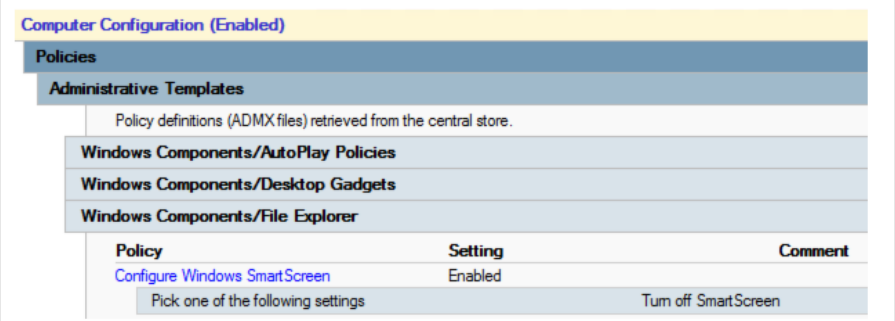
After the templates are upgraded, you see:



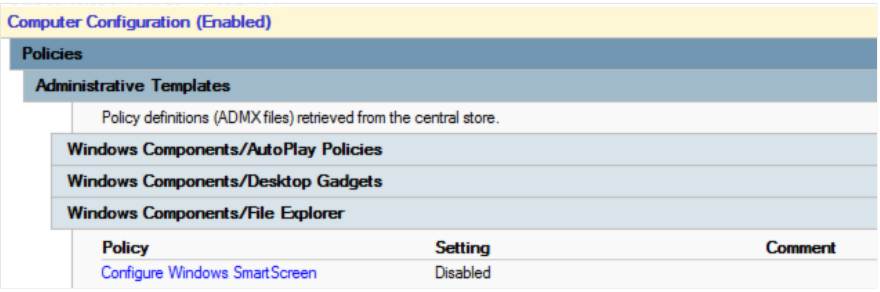
You now enable the policy and select to disable the smart screen, as shown:



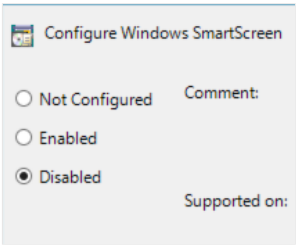
After you make this setting, you see the following in the report:



After you upgrade the templates to build 1607, the settings report reads as follows:



If you now edit the setting, you see:



Appendix 3 Windows Update

After the policy definitions are upgraded to at least the Windows 10 RTM build, and you configure the Windows Update settings to defer upgrades, you see:

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Windows Components/AutoPlay Policies

Windows Components/Desktop Gadgets

Windows Components/File Explorer

Windows Components/Internet Explorer/Internet Settings/Advanced settings/Search

Windows Components/Microsoft Edge

Windows Components/SkyDrive

Windows Components/Store

Windows Components/Windows Defender/Client Interface

Windows Components/Windows Error Reporting/Consent

Windows Components/Windows Update

Policy	Setting
Defer Upgrades and Updates	Enabled
Defer upgrades for the following duration (months):	3
Defer updates for the following duration (weeks):	4
Pause Upgrades and Updates	Enabled

After the PolicyDefinitions folder is upgraded to build 1611, the settings become extra registry settings, as shown:

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Windows Components/AutoPlay Policies

Windows Components/Desktop Gadgets

Windows Components/File Explorer

Windows Components/Internet Explorer/Internet Settings/Advanced settings/Sea

Windows Components/Microsoft Edge

Windows Components/SkyDrive

Windows Components/Store

Windows Components/Windows Defender/Client Interface

Windows Components/Windows Error Reporting/Consent

Extra Registry Settings

Display names for some settings cannot be found. You might be able to resolve this issue by

Setting	State
Software\Policies\Microsoft\MicrosoftEdge\Internet Settings\Zones\3\1400	0
Software\Policies\Microsoft\Windows\WindowsUpdate\DeferUpdatePeriod	4
Software\Policies\Microsoft\Windows\WindowsUpdate\DeferUpgrade	1
Software\Policies\Microsoft\Windows\WindowsUpdate\DeferUpgradePeriod	3
Software\Policies\Microsoft\Windows\WindowsUpdate\PauseDeferrals	1

Appendix 4 WinStoreUI upgrade to WindowsStore

Enabling the Microsoft Store options by using the Windows Server 2012 R2 build of ADMX provides the report:

Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Windows Components/AutoPlay Policies

Windows Components/Desktop Gadgets

Windows Components/File Explorer

Windows Components/Internet Explorer/Internet Settings/Ad

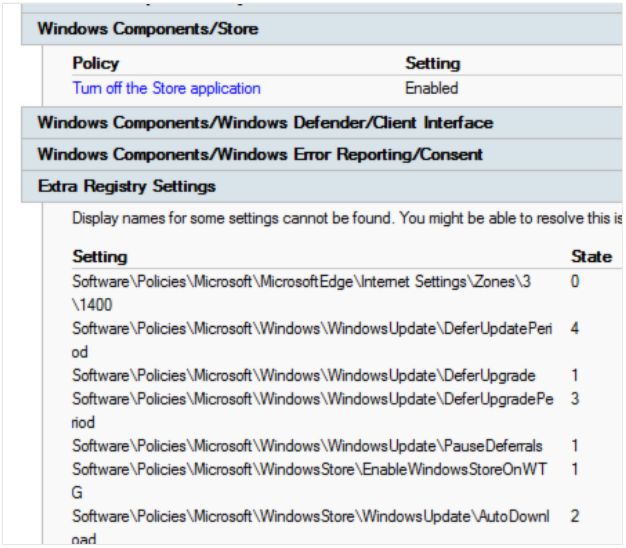
Windows Components/Microsoft Edge

Windows Components/SkyDrive

Windows Components/Store

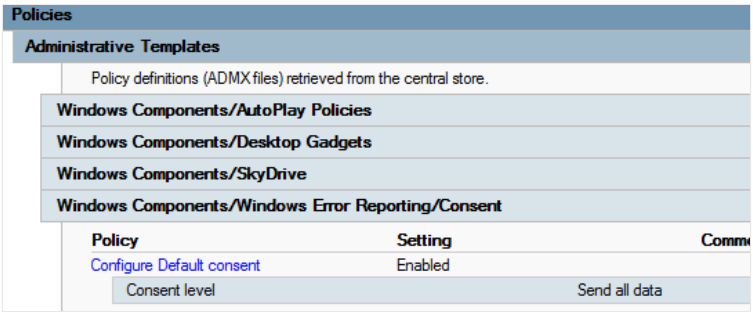
Policy	Setting
Allow Store to install apps on Windows To Go workspaces	Enabled
Turn off Automatic Download of updates	Enabled
Turn off the Store application	Enabled

After the ADMX files are replaced in the central store by build 1511, you see:

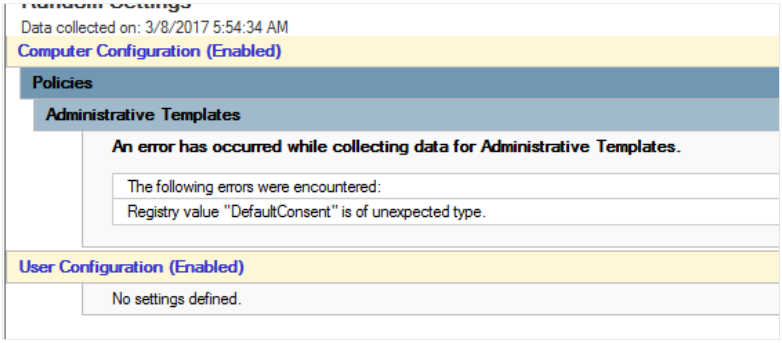


Appendix 5 Error reporting

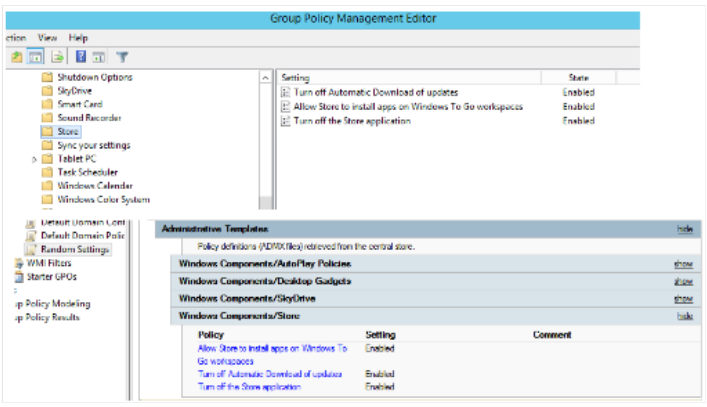
In Windows Server 2012 R2, you receive the following report if you enable **Configure Default consent**:



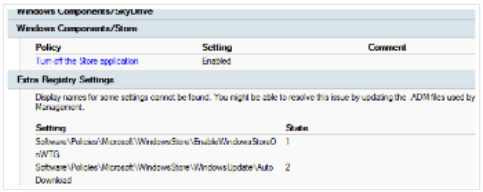
If errorreporting.admx is replaced, the report becomes as follows:



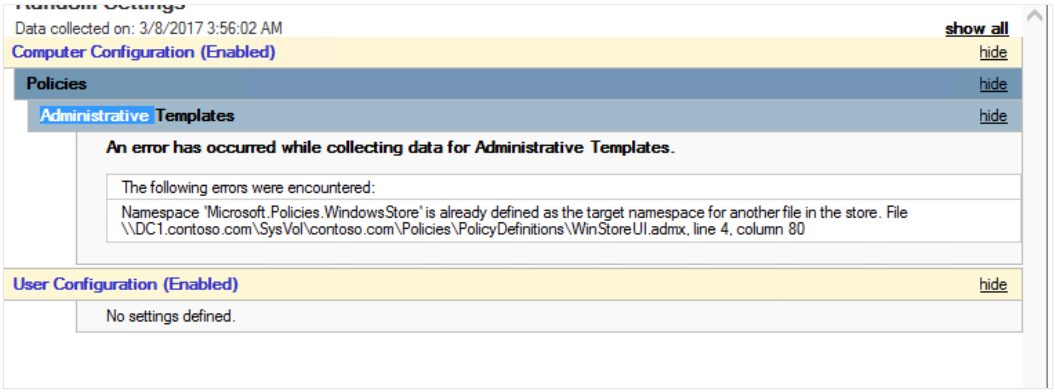
You can also see the image:



After WinStoreUI is removed and WindowsStore is added, you see:



After both ADMX/L templates are present in the policy definitions folder, you see:



The LsaLookupSids function may return the old user name instead of the new user name if the user name has changed

Article • 09/23/2021 • 2 minutes to read

This article describes a cache update delay in Windows.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 946358

Symptoms

Consider the following scenario:

- On the domain member computer, an application calls the **LsaLookupSids** function to translate a security identifier (SID) to a user name.
- The user name has been changed on a domain controller.

In this scenario, the **LsaLookupSids** function may return the old user name instead of the new user name. This behavior may prevent the application from working correctly.

Cause

The local security authority (LSA) caches the mapping between the SID and the user name in a local cache on the domain member computer. The cached user name isn't synchronized with domain controllers. The LSA on the domain member computer first queries the local SID cache. If an existing mapping is already in the local SID cache, the LSA returns the cached user name information instead of querying the domain controllers. This behavior is intended to improve performance.

The cache entries do time out, however chances are that recurring queries by applications keep the existing cache entry alive for the maximum lifetime of the cache entry.

Workaround

To work around this issue, disable the local SID cache on the domain member computer. To do this, follow these steps:

1. Open Registry Editor.

   To do this in Windows XP or in Windows Server 2003, click **Start**, click **Run**, type *regedit*, and then click **OK**.

   To do this in Windows Vista and newer, Click **Start**, type *regedit* in the **Start Search** box, and then press ENTER.

2. Locate and then right-click the following registry subkey:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`

3. Point to **New**, and then click **DWORD Value**.

4. Type LsaLookupCacheMaxSize, and then press ENTER.

5. Right-click **LsaLookupCacheMaxSize**, and then click **Modify**.

6. In the **Value data** box, type 0, and then click **OK**.

7. Exit Registry Editor.

> ⓘ **Note**
>
> The LsaLookupCacheMaxSize registry entry sets the maximum number of cached mappings that can be saved in the local SID cache. The default maximum number is 128. When the LsaLookupCacheMaxSize registry entry is set to 0, the local SID cache is disabled.

Status

The behavior is by design.

More information

The LSA maintains a SID cache on domain member computers. This cache stores mappings between SIDs and user names. If the SID information exists in the local cache, the LSA returns the cached user name information instead of checking whether the user name has changed.

The local SID cache helps reduce domain controller workload and network traffic. However, inconsistency may occur between the local cache and the domain controllers.

References

TechNet has an article that covers Sid-Name resolution approaches, including a detailed description of this cache:

How SIDs and Account Names Can Be Mapped in Windows

For more information about the **LsaLookupSids** function, visit the following Microsoft Web site:

LsaLookupSids function

UAC blocks the elevation of executable applications that are signed with revoked certificates

Article • 09/23/2021 • 2 minutes to read

This article describes new UAC behavior in Windows 10 that will disallow elevation of executable applications that are signed with revoked certificates.

Applies to: Windows 10 - all editions
Original KB number: 3082125

Summary

New User Account Control (UAC) behavior in Windows 10 disallows elevation of running applications that use revoked certificates to sign binary files.

More information

In Windows 10, UAC blocks executable binary files that are signed with revoked certificates.

This behavior prevents users from running certain applications. For example, users cannot run applications whose binary files are signed with stolen certificates.

To run an application, you must have the binaries files signed with valid certificates.

Windows Time service doesn't start automatically on a workgroup computer

Article • 09/23/2021 • 2 minutes to read

This article provides workarounds for an issue where the Windows Time service doesn't automatically start in a stand-alone environment.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2385818

Symptoms

On a workgroup computer that's running Windows 7, Windows Server 2008 R2, or a later version, the Windows Time service stops immediately after system startup. This issue occurs even after the Startup Type is changed from **Manual** to **Automatic**.

Cause

This issue occurs because the Windows Time service is configured as the Trigger-Start service, and it has been implemented as the default setting in Windows 7 and Windows Server 2008 R2.

Services and background processes have a significant effect on the performance of the system. The Trigger-Start service has been implemented in Windows 7 and Windows Service 2008 R2 to reduce the total number of auto-start services on the system. The goal is to improve the stability of the whole system, including improving performance and reducing power consumption. Under this implementation, the Service Control Manager has been enhanced to handle starting and stopping services by using specific system events.

For more information, see Service trigger events.

Whether the Windows Time service starts automatically depends on one of the following conditions:

- Whether the computer is joined to an Active Directory Domain Services (AD DS) domain environment.
- Whether the computer is configured as a workgroup computer.

The Windows Time service on domain-joined computers starts when a trigger event occurs. On workgroup computers that aren't joined to an AD DS domain:

- The startup value for the Windows Time service is **Manual**.
- The service status is **Stopped**.

You can check the Trigger-Start service settings by running the following command:

Console

```
sc qtriggerinfo w32time

Service Name: w32time

    Start Service
        DOMAIN JOINED STATUS: 1ce20aba-9851-4421-9430-1ddeb766e809 [DOMAIN
JOINED]

    Stop Service
        DOMAIN JOINED STATUS: ddaf516e-58c2-4866-9574-c3b615d42ea1 [NOT
DOMAIN JOINED]
```

Workaround

To start the Windows Time service at system startup, use any of the following methods.

- Method 1

  Run the `sc triggerinfo w32time delete` command to delete the trigger event that's registered as the default setting and to change the **Startup Type** setting for the Windows Time service from **Manual** to **Automatic**:

- Method 2

  Run the `sc triggerinfo w32time start/networkon stop/networkoff` command to define a trigger event that suits your environment. In this example, the command determines whether an IP address is given to a host. Then it starts or stops the service.

- Method 3

  Change the Startup Type of the Windows Time service from **Manual** to **Automatic (Delayed Start)**.

  > ⓘ **Note**

> If the Startup Type of the Windows Time service is set to **Automatic (Delayed Start)**, the Windows Time service may be started by the **Time Synchronization before the Service Control Manager starts the Windows Time service** task. It depends on the startup timing of the Windows operating system in question.

In this situation, the service triggers an automatic stop after the success of the Time Synchronization task. If you use Method 3, you must disable the **Time Synchronization to avoid the task to start the Windows Time service** task. To do so, follow these steps:

1. Start the Task Scheduler.
2. Under **Task Scheduler Library** > **Microsoft** > **Windows** > **Time Synchronization**, select **Synchronize Time**.
3. Right-click, and then select **Disabled** on the shortcut menu.

More information

The Windows Time service on a workgroup computer isn't started automatically at system startup by the Trigger-Start service. However, the Windows Time service is started by the Time Synchronization setting. The setting is registered on the Task Scheduler Library at 01:00 a.m. every Sunday for Time Synchronization. So the default setting can be kept as is.

Admin Development troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Admin Development-related issues. Browse the content or use the search feature to find relevant content.

Admin Development sub category

- Active Directory Services Interface (ADSI)

User authentication issues with the Active Directory Service Interfaces WinNT provider

Article • 09/23/2021 • 2 minutes to read

This article describes user authentication issues with Active Directory Service Interfaces (ADSI) WinNT provider.

Applies to: Windows 10 - all editions
Original KB number: 218497

Summary

The **ADSI OpenDsObject** method or the **ADsOpenDsObject C helper** function allows you to provide authentication credentials to the directory server when you open an object. There are a number of issues that you should be aware of when you use this technique with the Active Directory Service Interfaces WinNT provider.

More information

The Active Directory Service Interfaces WinNT provider uses the **WNetAddConnection2** function to make a connection to \\servername\IPC$ in order to establish these credentials with the remote server. This method is useful because it doesn't require special privileges for NT clients and it works on Windows and it supports authentication across untrusted domains.

Unfortunately, there are several drawbacks inherent in the **WNetAddConnection2** function, and they are as follows:

- If any connection has already been established to the target server by any process running on the client computer, the **WNetAddConnection2** function cannot make a new connection under any credentials other than those used for the existing connection.

  If you try to authenticate a new account, you will get a conflicting credentials error. If you try to authenticate the existing account, any password will work (valid or not). This is a particular problem when you are getting objects from a domain controller where many system processes establish connections to domain controllers.

- If the Guest account is enabled on the destination computer, it is possible to pass both an invalid username and password and to create a connection.
- The system does not reference count connections, thus, if any process, including your Active Directory Service Interfaces client process, deletes the connection, then all processes using that connection have to be written to re-establish it when they find it has been deleted.

When you are using the WinNT provider, we recommend that you authenticate with the target server by logging on to a domain account with appropriate credentials or using the **LogonUser** function (which requires elevated privileges) prior to executing your Active Directory Service Interfaces code. We also recommend that you do not use the Active Directory Service Interfaces OpenDsObject method to validate a user's credentials on any domain that is trusted by your client computer.

If you are attempting to validate accounts from untrusted domains, use the Active Directory Service Interfaces OpenDsObject method, keeping the issues listed above in mind and understanding that you will be sending unencrypted passwords over the network. You can overcome these restrictions by running validation code as a service on at least one server in each set of untrusted domains using an SSL (or HTTPS) connection to provide encryption. Accomplish this by using a validation .asp file on an IIS server in each set of untrusted domains and connect to it over HTTPS using basic authentication.

The Active Directory Service Interfaces OpenDsObject method uses the credentials of the logged on user to access IIS. The user name and the password that are given as parameters are ignored. You receive the following error message:

> Access Denied

However, it works after the logged on user of the client is added to the Administrators group of the server.

It also works if you use the following script code.

Visual Basic Script

```
Set objLogon = CreateObject("LoginAdmin.ImpersonateUser")
objLogon.Logon "Administrator", "AdminPassword", "Machinename"
Set oNS = GetObject("IIS:")
Set oRoot = oNS.OpenDSObject("IIS://SERVER/SHARE", "Mordor\administrator",
"Gollum", 1)'User credentials are ignored
objLogon.Logoff
Set objLogon = Nothing
```

How to create a desktop shortcut with the Windows Script Host

Article • 09/23/2021 • 2 minutes to read

This article describes how to create desktop shortcuts by using the Microsoft Windows Script Host (WSH) from within Visual FoxPro.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 244677

Summary

The WSH is a tool that allows you to run Microsoft Visual Basic Scripting Edition and JScript natively within the base Operating System, either on Windows 95 or Windows NT 4.0. It also includes several COM automation methods that allow you to do several tasks easily through the Windows Script Host Object Model. The Microsoft Windows Script Host is integrated into Windows 98, Windows 2000, and later versions of the Windows operating system. It is available for Windows NT 4.0 by installing the Windows NT 4.0 Option Pack. To download this tool, visit Scripting.

Examples to create a desktop shortcut with WSH

This program demonstrates how to use the Windows Script Host to create a shortcut on the Windows Desktop. In order to run this example, you must have the Windows Script Host installed on your computer. To run one of these examples, copy the code below into a new program file and run it.

Example 1

Visual Basic Script

```
WshShell = CreateObject("Wscript.shell")
strDesktop = WshShell.SpecialFolders("Desktop")
oMyShortcut = WshShell.CreateShortcut(strDesktop + "\Sample.lnk")
oMyShortcut.WindowStyle = 3 &&Maximized 7=Minimized 4=Normal
oMyShortcut.IconLocation = "C:\myicon.ico"
OMyShortcut.TargetPath = "%windir%\notepad.exe"
oMyShortCut.Hotkey = "ALT+CTRL+F"
oMyShortCut.Save
```

Example 2: Add a command-line argument

Visual Basic Script

```
WshShell = CreateObject("WScript.Shell")
strDesktop = WshShell.SpecialFolders("Desktop")
oMyShortCut= WshShell.CreateShortcut(strDesktop+"\Foxtest.lnk")
oMyShortCut.WindowStyle = 7 &&Minimized 0=Maximized 4=Normal
oMyShortcut.IconLocation = home()+"wizards\graphics\builder.ico"
oMyShortCut.TargetPath = "c:\Program Files\Microsoft Visual
Studio\VFP98\vfp6.exe"
oMyShortCut.Arguments = '-c'+'"'+Home()+'config.fpw'+'"'
oMyShortCut.WorkingDirectory = "c:\"
oMyShortCut.Save
```

> ⓘ Note
>
> Depending on the version of Visual FoxPro that you are using, you may need to change the name and the path of the Visual FoxPro executable in Example 2.

Example 3: Add a URL shortcut to the desktop

Visual Basic Script

```
WshShell = CreateObject("WScript.Shell")
strDesktop = WshShell.SpecialFolders("Desktop")
oUrlLink = WshShell.CreateShortcut(strDesktop+"\Microsoft Web Site.URL")
oUrlLink.TargetPath = "http://www.microsoft.com"
oUrlLink.Save
```

> ⓘ Note
>
> For the shortcut to be created, valid parameters must be passed for all methods. No error appears if one of the parameters is incorrect.

References

- White paper: Windows Script Host: A universal Scripting Host for scripting languages
- Technical paper: Windows Script Host programmer's reference

Application Management documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Application Management-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Application Management sub categories

- .NET Framework installation
- First Party Applications
- COM and COM+ performance and stability
- DCOM service startup and permissions
- Modern, Inbox, and Microsoft Store Apps
- MSI
- Multilingual User Interface (MUI) and Input Method Editor (IME)
- Windows Script Host (`CScript` or `WScript`)

.NET Framework 3.5 installation errors: 0x800F0906, 0x800F081F, 0x800F0907, 0x800F0922

Article • 03/24/2022 • 10 minutes to read

This article helps fix Microsoft .NET Framework 3.5 installation errors.

Applies to: Windows 10 - all editions, Windows Server 2019, Windows Server 2012 R2
Original KB number: 2734782

> **Note**
>
> Installation of the .NET Framework may throw errors that are not listed in this article, but you might be able to try the following steps to fix those errors as well. Microsoft is releasing Out-of-band (OOB) updates for .NET Framework. **.NET Framework Out-of-band update to address issues after installing the January 11, 2022 Windows update**

Resolutions for Windows Server

You may receive the following errors when you install the .NET Framework 3.5 in Windows Server:

- Error code 0x800F0906
- Error code 0x800F081F
- Error code 0x800F0907

Error code 0x800F0906

This error code occurs because the computer cannot download the required files from Windows Update.

To resolve this issue, use one of the following methods:

Method 1: Check your internet connection

This behavior can be caused by network, proxy, or firewall configurations or by network, proxy, or firewall failures. To fix this problem, try to connect to the Microsoft Update

website.

If you cannot access this website, check your Internet connection, or contact the network administrator to determine whether there is a configuration that blocks access to the website.

Method 2: Configure the Group Policy setting

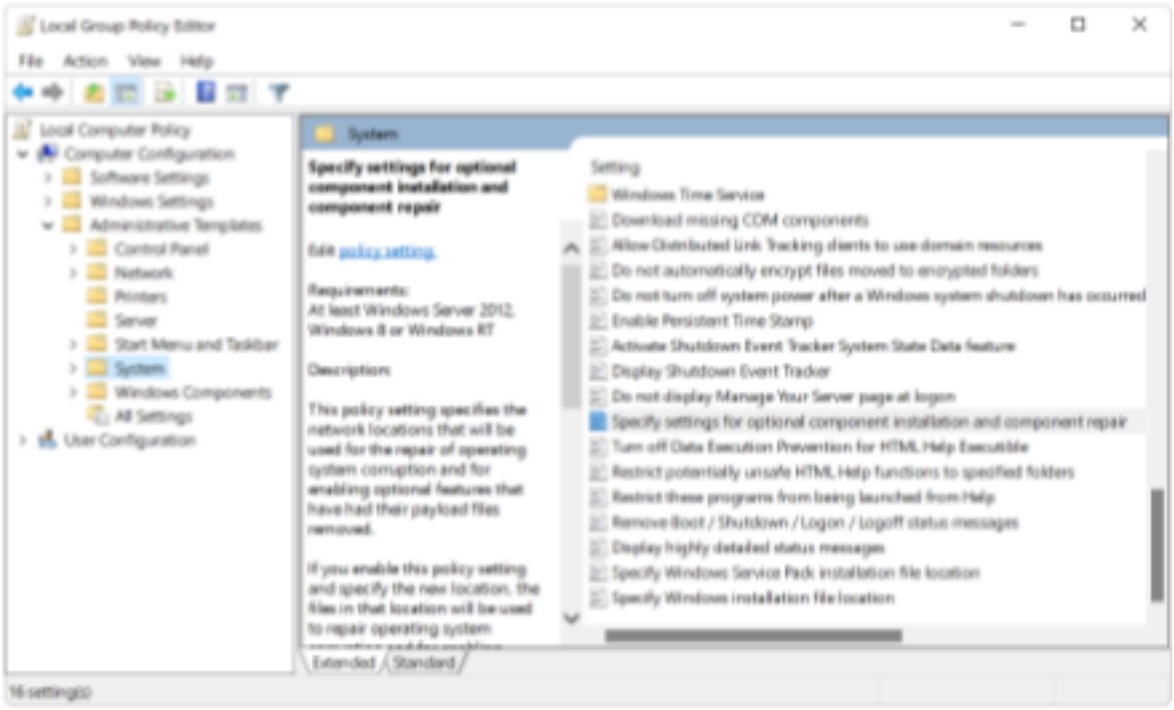
This behavior can also be caused by a system administrator who configures the computer to use Windows Server Update Services (WSUS) instead of the Windows Update server for servicing. In this case, contact your system administrator and request that they enable the **Specify settings for optional component installation and component repair** Group Policy setting and configure the **Alternate source file path** value or select the **Contact Windows Update directly to download repair content instead of Windows Server Update Services (WSUS)** option.

To configure the Group Policy setting, follow these steps:

1. Start the Local Group Policy Editor or Group Policy Management Console.

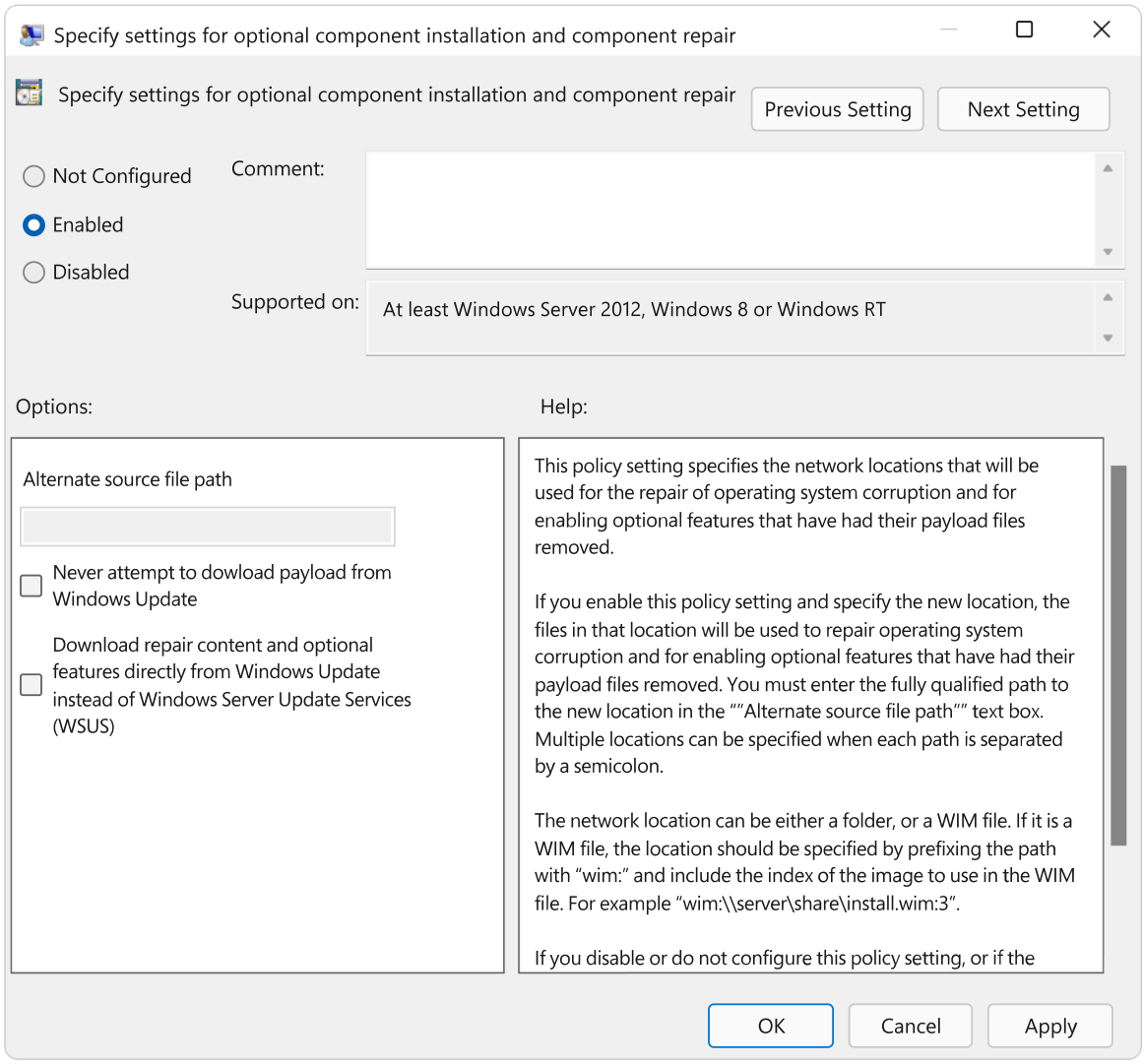
   Point to the upper-right corner of the screen, click **Search**, type group policy, and then click **Edit group policy**.

2. Expand **Computer Configuration**, expand **Administrative Templates**, and then select **System**. The screenshot for this step is listed below.



3. Open the **Specify settings for optional component installation and component repair** Group Policy setting, and then select **Enabled**. The screenshot for this step is

listed below.



4. If you want to specify an alternative source file, in the **Alternate source file path** box, specify a fully qualified path of a shared folder that contains the contents of the `\sources\sxs` folder from the installation media.

   Example of a shared folder path: `\\server_name\share\Win8sxs`

   Or, specify a WIM file. To specify a WIM file as an alternative source file location, add the prefix **WIM:** to the path, and then add the index of the image that you want to use in the WIM file as a suffix.

   Example of a WIM file path: `WIM:\\server_name\share\install.wim:3`

> **Note**
>
> In this example, `3` represents the index of the image in which the feature files are found.

5. If it is applicable to do this, select the **Contact Windows Update** directly to download repair content instead of **Windows Server Update Services (WSUS)** check box.
6. Tap or click **OK**.
7. At an elevated command prompt, type `gpupdate /force`, and then press **Enter** to apply the policy immediately.

Method 3: Use Windows installation media

You can use the Windows installation media as the file source when you enable the .NET Framework 3.5 feature. To do this, follow these steps:

1. Insert the Windows installation media.
2. At an elevated command prompt, run the following command:

   Console

   ```
   Dism /online /enable-feature /featurename:NetFx3 /All /Source:
   <drive>:\sources\sxs /LimitAccess
   ```

   In this command, <drive> is a placeholder for the drive letter for the DVD drive. For example, you run the following command:

   Console

   ```
   Dism /online /enable-feature /featurename:NetFx3 /All
   /Source:D:\sources\sxs /LimitAccess
   ```

Method 4: Alternative steps for Windows Server

In Windows Server 2012 R2, you can also specify an alternative source by using Windows PowerShell cmdlets or by using the **Add Roles and Features Wizard**.

To use Windows PowerShell, follow these steps:

1. Insert the Windows installation media.
2. In an elevated Windows PowerShell command window, run the following command:

   PowerShell

```
Install-WindowsFeature name NET-Framework-Core source
<drive>:\sources\sxs
```

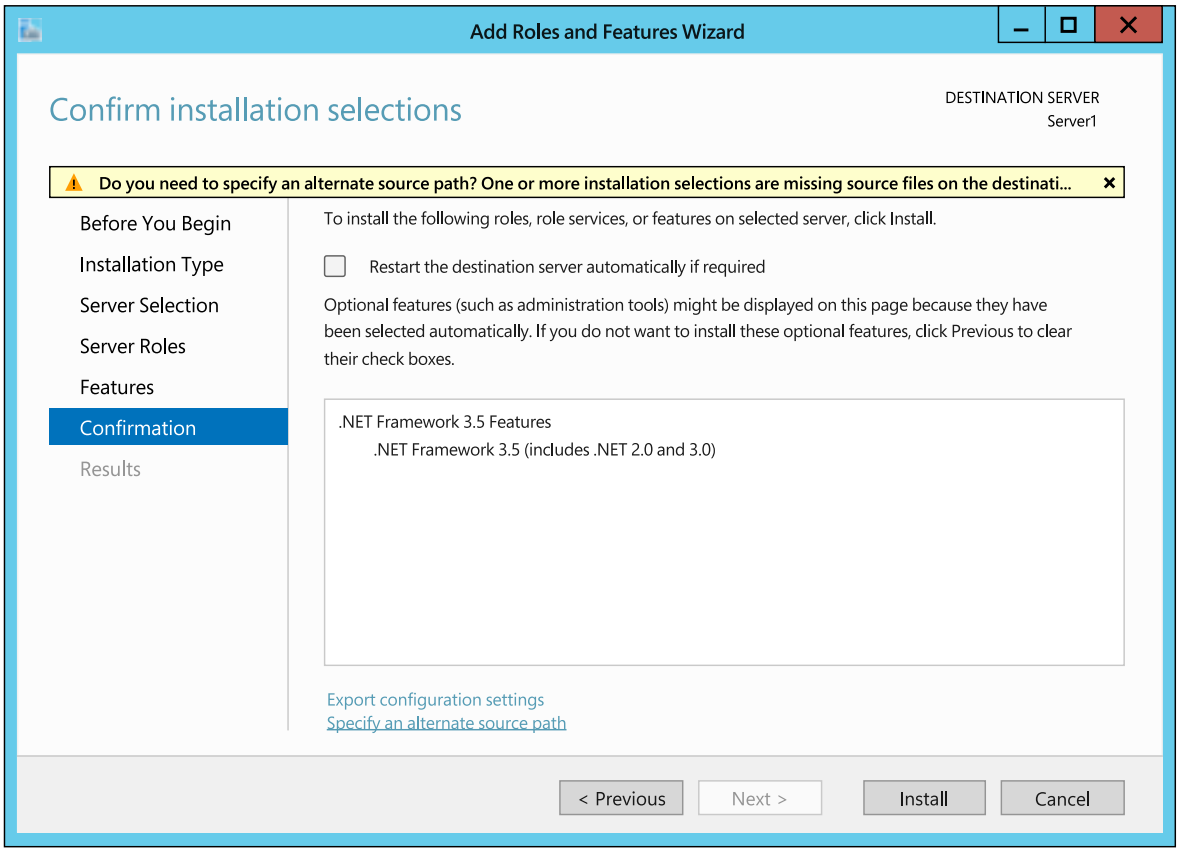
In this command, <drive> is a placeholder for the drive letter for the DVD drive or for the Windows installation media. For example, you run the following command:

PowerShell

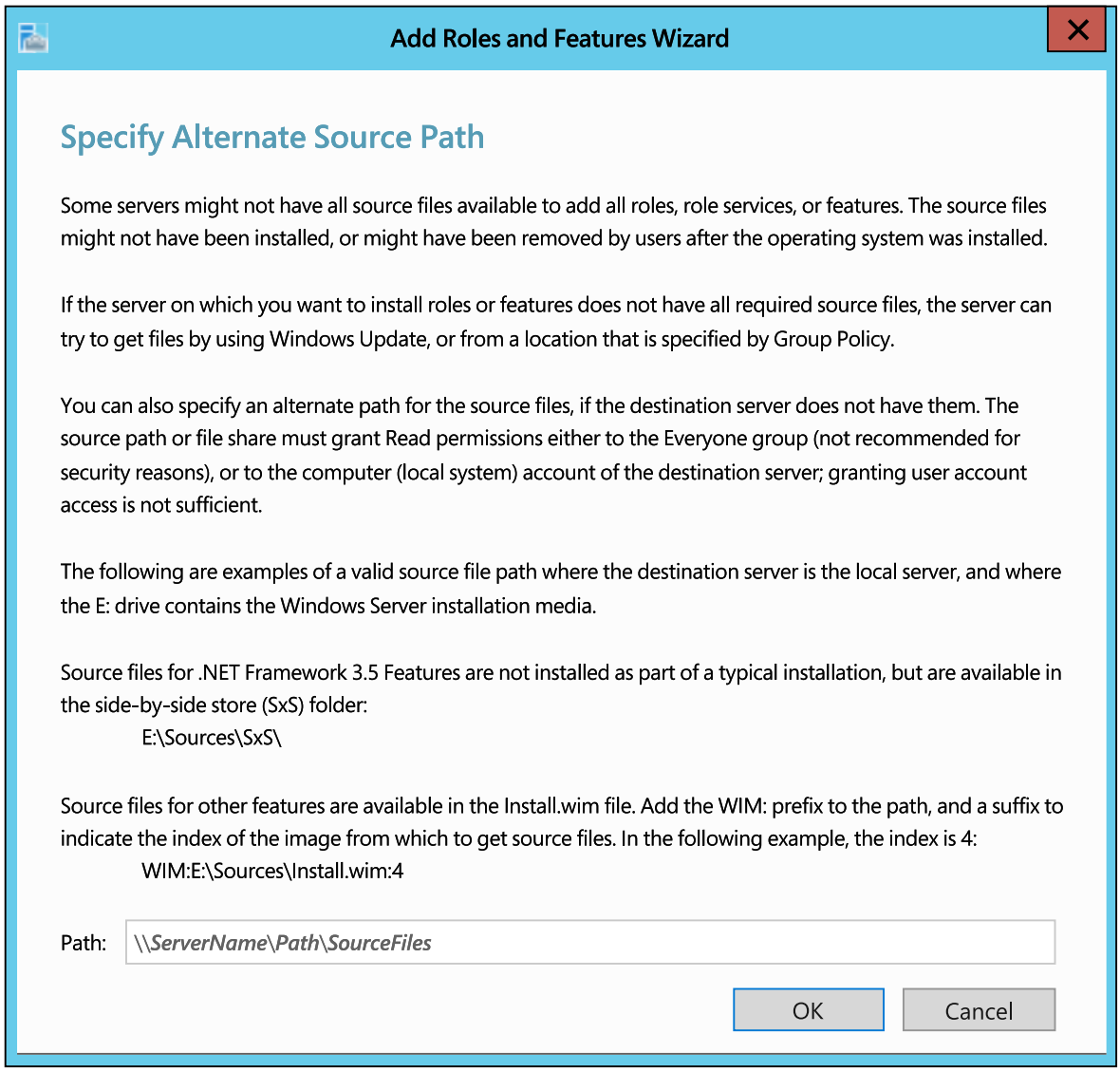
```
Install-WindowsFeature name NET-Framework-Core source D:\sources\sxs
```

To use the **Add Roles and Features Wizard**, follow these steps:

1. Insert the Windows installation media.
2. Start the **Add Roles and Features Wizard**.
3. On the **Select features** page, select the **.NET Framework 3.5 Features** check box, and then click **Next**.
4. On the **Confirm installation selections** page, click the **Specify an alternate source path** link. The screenshot for this step is listed below.



5. On the **Specify Alternate Source Path** page, type the path of the *SxS* folder as a local path or as a network share path. The screenshot for this step is listed below.



6. Click **OK**.

7. Click **Install** to finish the wizard.

Error code 0x800F081F

This error code can occur when an alternative installation source is specified and one of the following conditions is true:

- The location that is specified by the path does not contain the files that are required to install the feature.
- The user who tries to install the feature does not have at least READ access to the location and to the files.
- The set of installation files is corrupted, incomplete, or invalid for the version of Windows that you are running.

To fix this problem, make sure that the full path of the source is correct (`x:\sources\sxs`) and that you have at least Read access to the location. To do this, try to access the source directly from the affected computer. Verify that the installation source contains a

valid and complete set of files. If the problem persists, try to use a different installation source.

Error code 0x800F0907

This error code occurs if an alternative installation source is not specified or is invalid and if the **Specify settings for optional component installation and component repair** Group Policy setting is configured to **Never attempt to download payload from Windows Update**.

To fix this problem, review the policy setting to determine whether it is appropriate for your environment. If you do not want to download feature payloads from Windows Update, consider configuring the **Alternate source file path** value in the Group policy setting.

> ⓘ **Note**
>
> You must be a member of the Administrators group to change Group Policy settings on the local computer. If the Group Policy settings for the computer that you want to manage are controlled at the domain level, contact your system administrator.

To do this, follow these steps:

1. Start Local Group Policy Editor or Group Policy Management Console as applicable in your environment.
2. Expand **Computer Configuration**, expand **Administrative Templates**, and then select **System**.
3. Open the **Specify settings for optional component installation and component repair** Group Policy setting, and then select **Enabled**.
4. Determine whether the **Never attempt to download payload from Windows Update** Group Policy setting is enabled, and then determine the desired setting for your environment.
5. If you want to specify an alternate source file, in the **Alternate source file path** box, specify a fully qualified path of a shared folder that contains the contents of the `\sources\sxs` folder from the installation media. Or, specify a WIM file. To specify a WIM file as an alternative source file location, add the prefix **WIM:** to the path, and

then add the index of the image that you want to use in the WIM file as a suffix. The following are examples of values that you can specify:

- Path of a shared folder: `\\server_name\share\Win8sxs`
- Path of a WIM file, in which `3` represents the index of the image in which the feature files are found: `WIM:\\server_name\share\install.wim:3`

6. If you want, select the **Contact Windows Update directly to download repair content instead of Windows Server Update Services (WSUS)** check box.
7. Tap or click **OK**.
8. At an elevated command prompt, type the `gpupdate /force`, and then press **Enter** to apply the policy immediately.

Resolution for Windows 10

- **Error code 0x800F0906, 0x800F081F, or 0x800F0907**

  To fix the error codes for Windows 10, follow these steps:

  1. Download the Windows Media Creation tool, and create an ISO image locally, or create an image for the version of Windows that you have installed.
  2. Configure the Group Policy as in Method 2, but also follow these steps:
     a. Mount the ISO image that's created in step 1.
     b. Point the **Alternate source file path** to the ISO `sources\sxs` folder from the ISO.
     c. Run the `gpupdate /force` command.
     d. Add the .NET Framework feature.

- **Error code 0x800F0922**

  The following error message occurs when you do Windows 10 upgrade:

  > 0x800F0922 CBS_E_INSTALLERS_FAILED: Processing advanced installers and generic commands failed.

  > **Note**
  >
  > This error code is not specific to .NET Framework.

To fix this issue, follow these steps:

1. Open the .NET Framework installation files folder.
2. Open *Sources* folder.
3. Right-click the *SXS* folder, and then click **Properties**.
4. Click **Security** and make sure that there is a check mark next to **Read & Execute**. If the check mark isn't there, click the **Edit** button and turn it on.
5. Press Windows Key + X keyboard shortcut.
6. Click **Command Prompt (Admin)**.
7. In the **Command Prompt** window, type the following command and press Enter:

   ```
   Console

   dism /online /enable-feature /featurename:netfx3 /all
   /source:c:\sxs /limitaccess
   ```

8. In the **Command Prompt** window, type the following command and press Enter:

   ```
   Console

   dism /online /Cleanup-Image /RestoreHealth
   ```

More information

These errors may occur when you use an installation wizard, the Deployment Image Servicing and Management (DISM) tool, or Windows PowerShell commands to enable the .NET Framework 3.5.

In Windows 10 and Windows Server 2012 R2, the .NET Framework 3.5 is a Feature on Demand. The metadata for Features on Demand is included. However, the binaries and other files associated with the feature are not included. When you enable a feature, Windows tries to contact Windows Update to download the missing information to install the feature. The network configuration and how computers are configured to install updates in the environment can affect this process. Therefore, you may encounter errors when you first install these features.

Error messages that are associated with these error codes

Error code	Error messages
0x800F0906	The source files could not be downloaded. Use the **source** option to specify the location of the files that are required to restore the feature. For more information on specifying a source location, see `http://go.microsoft.com/fwlink/?LinkId=243077`. The DISM log file can be found at C:\Windows\Logs\DISM\dism.log. Windows couldn't complete the requested changes. Windows couldn't connect to the Internet to download necessary files. Make sure that you're connected to the Internet, and click **Retry** to try again. Installation of one or more roles, role services, or features failed. The source files could not be found. Try installing the roles, role services, or features again in a new Add Roles and Features Wizard session, and on the Confirmation page of the wizard, click **Specify an alternate source path** to specify a valid location of the source files that are required for the installation. The location must be accessible by the computer account of the destination server. 0x800F0906 - CBS_E_DOWNLOAD_FAILURE Error code: 0x800F0906 Error: 0x800f0906
0x800F081F	The source files could not be found. Use the **Source** option to specify the location of the files that are required to restore the feature. For more information on specifying a source location, see `http://go.microsoft.com/fwlink/?LinkId=243077`. The DISM log file can be found at C:\Windows\Logs\DISM\dism.log 0x800F081F - CBS_E_SOURCE_MISSING Error code: 0x800F081F Error: 0x800F081F

Error code	Error messages
0x800F0907	DISM failed. No operation was performed. For more information, review the log file. The DISM log file can be found at C:\Windows\Logs\DISM\dism.log Because of network policy settings, Windows couldn't connect to the Internet to download files that are required to complete the requested changes. Contact your network administrator for more information. 0x800F0907 - CBS_E_GROUPPOLICY_DISALLOWED Error code: 0x800F0907 Error: 0x800F0907

Download the .NET Framework 3.5 outside of the Windows Update requirement

The .NET Framework 3.5 is available for customers with Volume Licensing or MSDN Subscription, as Feature on-Demand Media is available.

Error codes are not listed when you install .NET Framework 3.5

When you install .NET Framework 3.5, you may encounter other error codes that are not listed in this article, for more information, go to the following articles:

- Windows help
- Net Framework 3.5 and 4.5 error 0x80070002
- Install the .NET Framework 3.5 in Windows 10
- Microsoft .NET Framework 3.5 Deployment Considerations

Performance of System.Diagnostics.StackFrame decreases in Windows 10 and .NET Framework 4.7.1

Article • 04/12/2022 • 3 minutes to read

This article helps fix an issue where applications that use `System.Diagnostics.StackFrame` run slower than before after you upgrade to Windows 10 or Microsoft .NET Framework 4.7.1.

Applies to: Windows 10, version 1803, Windows 10, version 1709
Original KB number: 4057154

Symptoms

Starting in October 2017, after you upgrade to Windows 10 or .NET Framework 4.7.1, you notice a significant decrease in performance when you run .NET Framework applications that use the `System.Diagnostics.StackFrame` class.

Applications typically rely on `StackFrame` when they throw .NET exceptions. If this occurs at a high rate (more than 10 incidents per second), applications can slow down significantly (tenfold) and run noticeably slower than before.

To determine your version of Windows, see Which Windows operating system am I running? .

Resolution

This issue is fixed in the following Windows updates.

- For Windows 10 Version 1709

  January 31, 2018-KB4058258 (OS Build 16299.214)

- For all other supported Windows versions

  .NET Framework 4.7.1 Update (KB4054856)

To work around this issue, use one of the following methods.

Workaround 1 (preferred): Use a different constructor for StackFrame that takes a Boolean argument

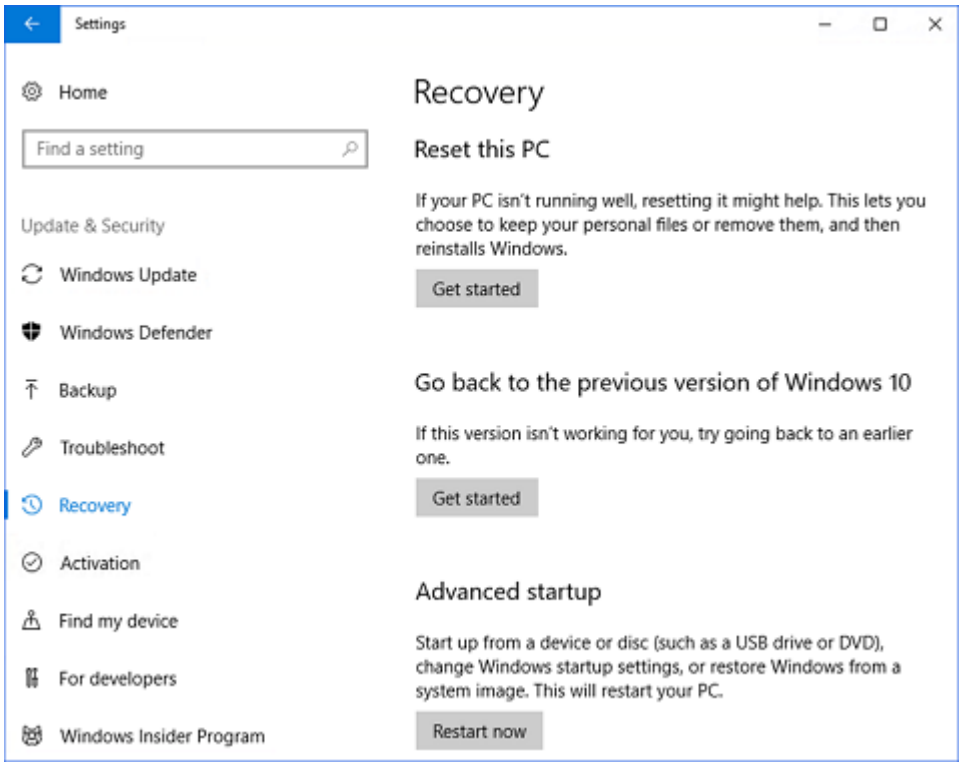
If application developers are able to make changes to their applications, call the `System.Diagnostics.StackTrace.#ctor(Boolean)` constructor by using a false argument to avoid capturing source information. This avoids the section of the code in which performance is decreased.

Workaround 2: Roll back the system version

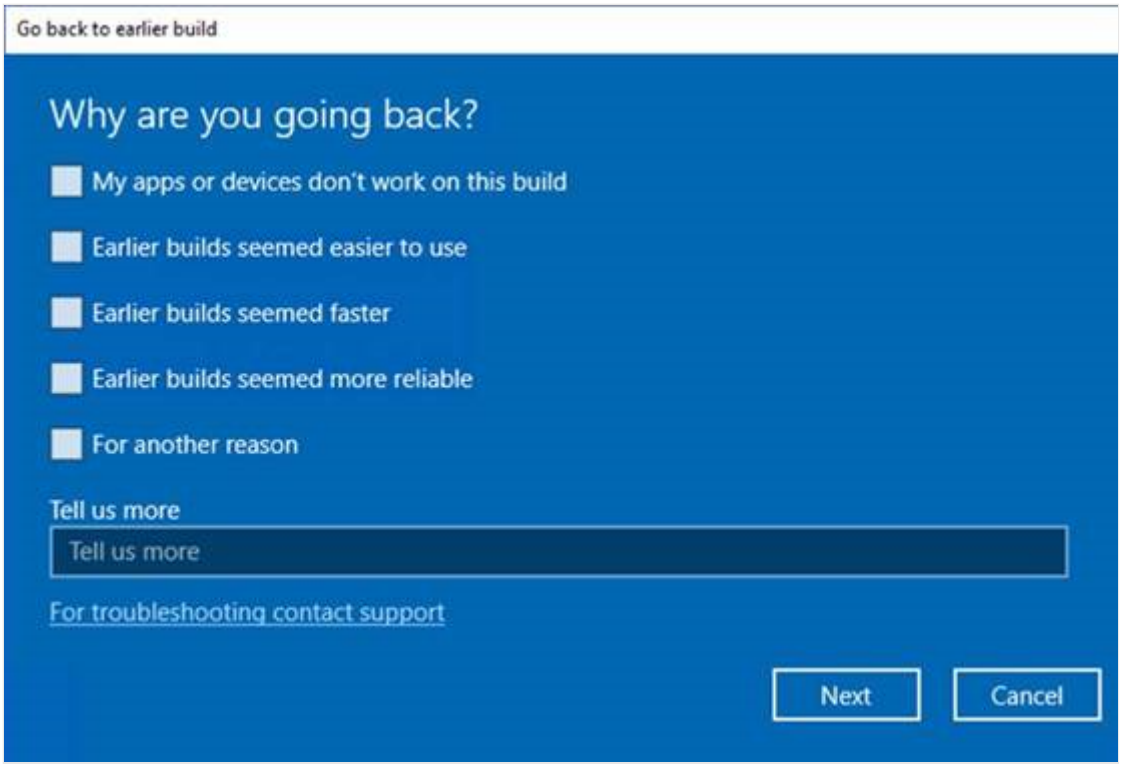
Roll back the system to the previous version of Windows 10 or .NET Framework. To do this, follow these steps.

How to roll back to the previous version of Windows 10

1. Open **Settings**, select **Update & Security**, and then select **Recovery**.
2. Under **Go back to the previous version of Windows 10**, select **Get started**.



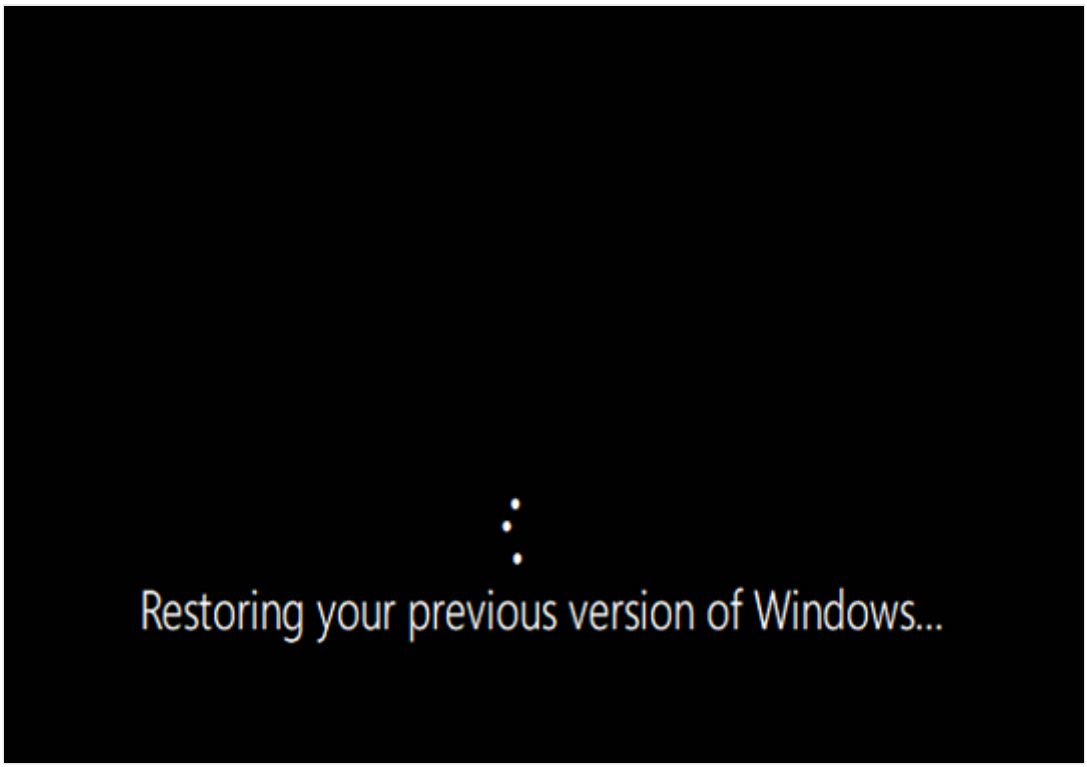
3. Select a reason for rolling back, and then select **Next**.



4. Select **No, thanks** to skip installing updates.

5. Select **Next** two times, and then select **Go back to earlier build**.

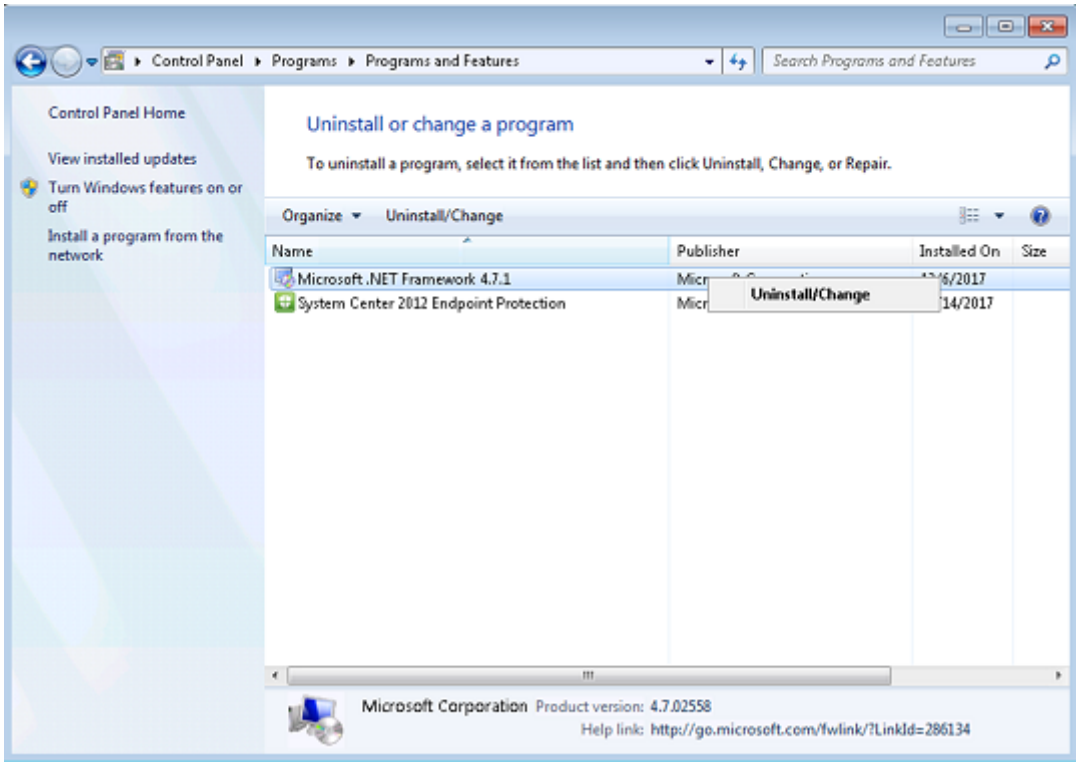
After you complete these steps, Windows 10 restores the previous version of the system.



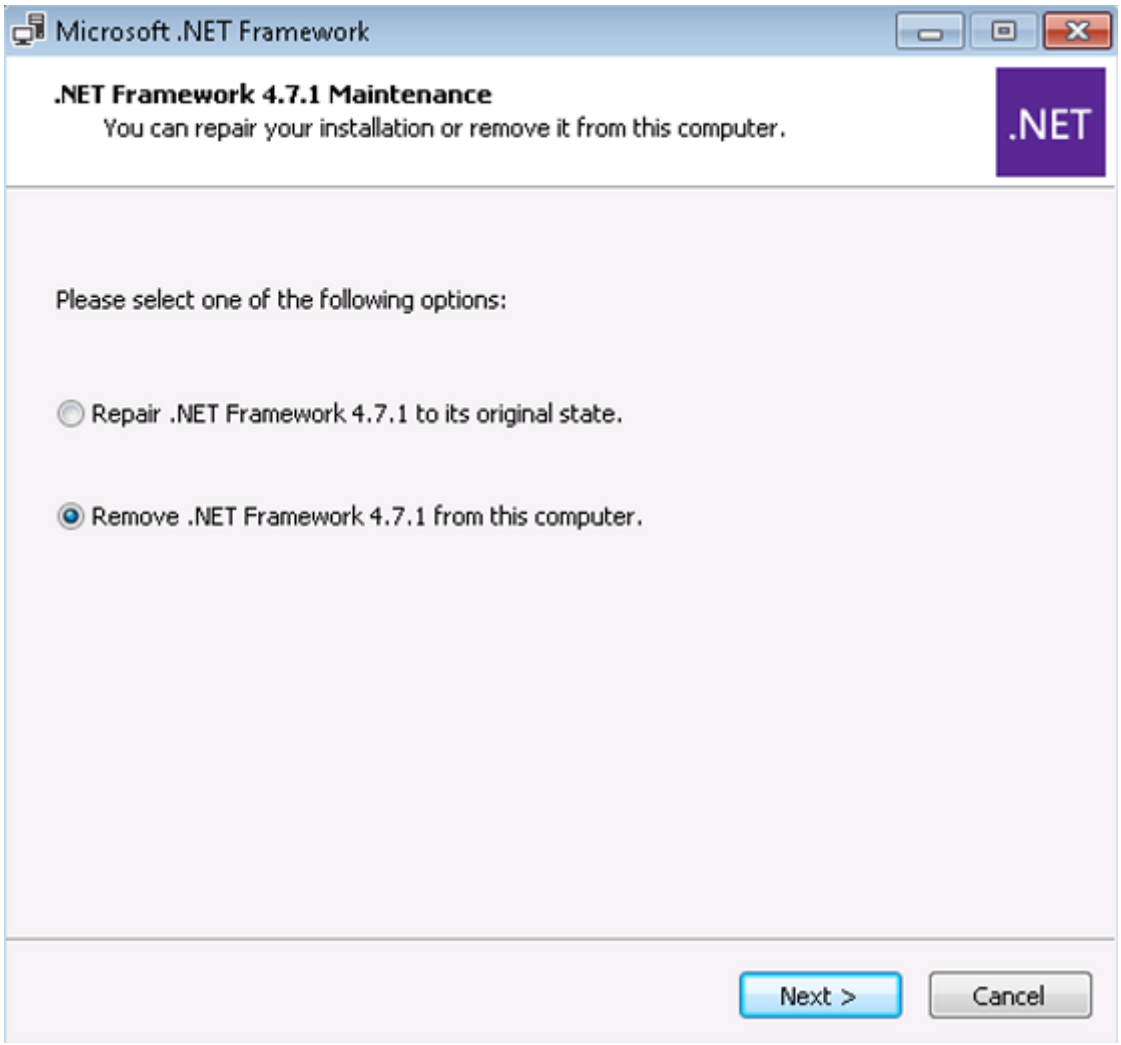
How to roll back to the previous version of .NET Framework

Steps for Windows 7 SP1 and Windows Server 2008 R2 SP1:

1. Open the **Programs and Features** item in Control Panel.
2. In the **Uninstall or change a program** list, locate and select **Microsoft .NET Framework 4.7.1**, and then select **Uninstall/Change**.

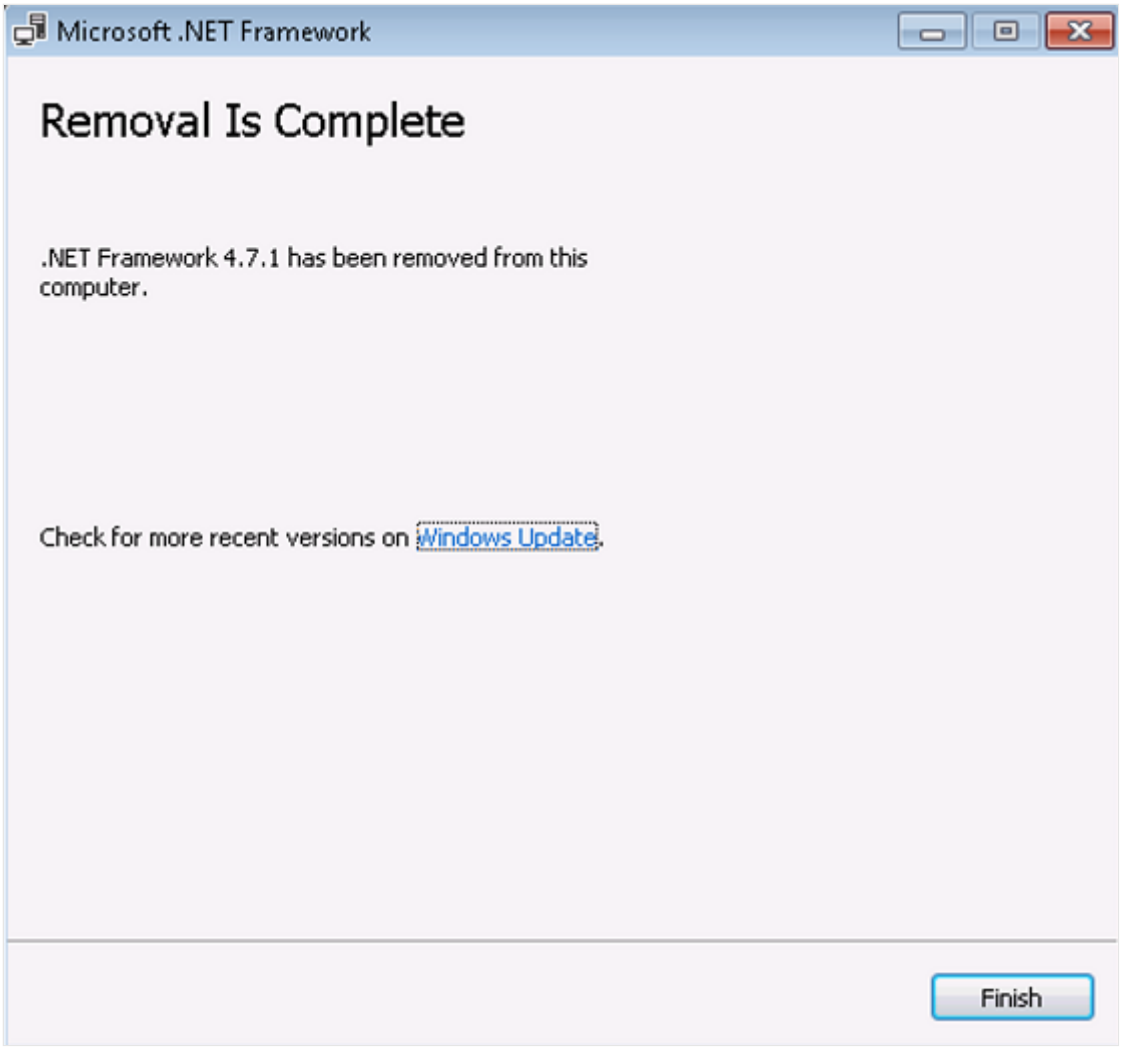


3. Select **Remove .NET Framework 4.7.1 from this computer**, and then select **Next**.



4. Select **Continue** to confirm uninstallation.

5. Select **Finish** after the uninstallation is finished.



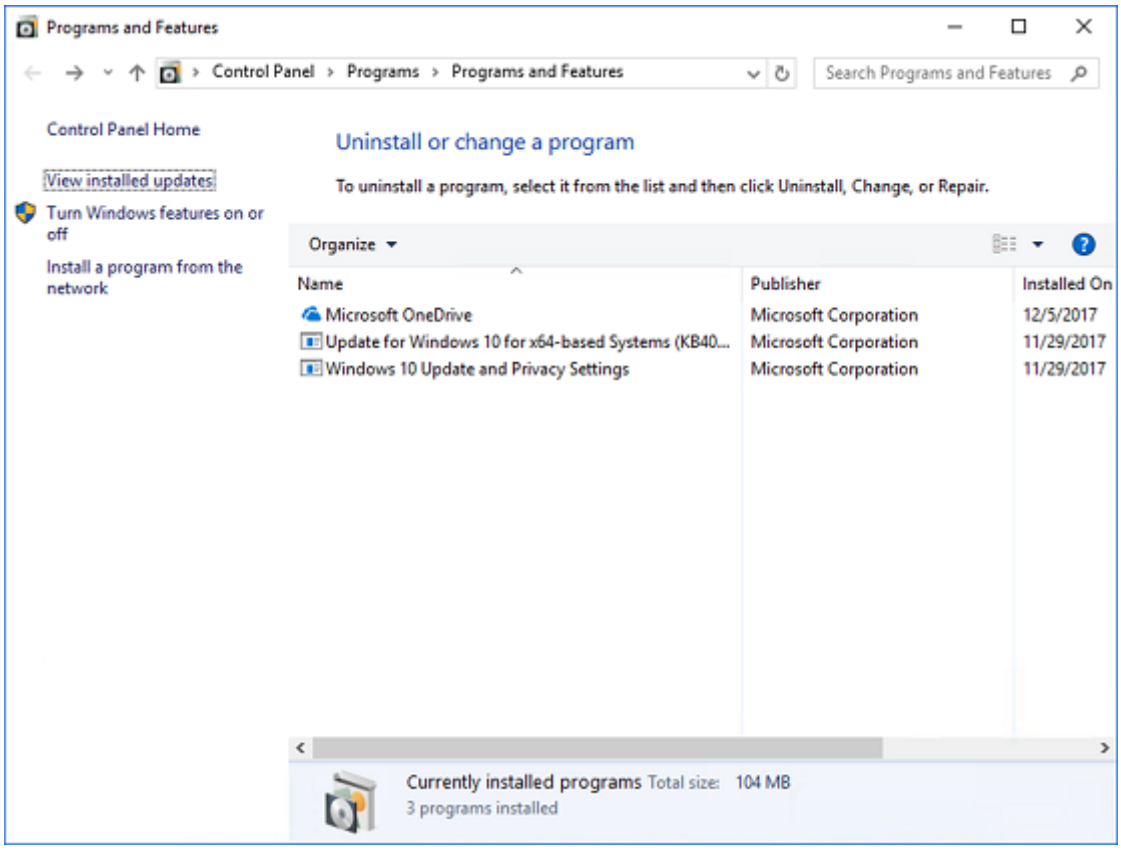
6. Restart your computer if you are prompted to do this.

> ⓘ **Note**
>
> After you uninstall .NET Framework 4.7.1, your computer no longer has any version of .NET Framework 4 installed. You must reinstall a version of .NET Framework 4.

Steps for Windows 8.1, Windows Server 2012, Windows Server 2012 R2, and Windows 10 Version 1607:

1. Open the **Programs and Features** item in Control Panel. To do this, type *appwiz.cpl* in the **Search** box.

2. Select **View installed updates**.



3. Right-click one of the following items, depending on your Windows version, and then click **Uninstall**:

   - Windows Server 2012: **Update for Microsoft Windows (KB4033345)**
   - Windows 8.1 or Server 2012 R2: **Update for Microsoft Windows (KB4033369)**
   - Windows 10 Version 1607: **Update for Microsoft Windows (KB4033369)**

4. Click **Yes** to confirm uninstallation.

5. Restart your computer if you are prompted to do this.

More information

For more information about how many .NET exceptions a particular application throws, see Exception Performance Counters.

For more information about how to measure the rate of exceptions for an application, see Runtime Profiling.

> ⓘ **Note**
>
> This issue does not change the number of exceptions that are thrown. However, it does significantly decrease the ability of applications to handle those exceptions.

For more information about this issue, see **this GitHub post**.

Applications that use IKVM library are known to be affected by this issue if they probe for assemblies. Probing for assemblies is known to cause exceptions.

64-bit versions of Windows don't support 16-bit components, 16-bit processes, or 16-bit applications

Article • 09/23/2021 • 2 minutes to read

This article discusses the lack of support for 16-bit components, 16-bit processes, or 16-bit applications in x64-based versions Windows.

Applies to: Window 10 – all editions, Windows Server 2012 R2
Original KB number: 896458

Summary

The x64-based versions of Windows don't support 16-bit programs, 16-bit processes, or 16-bit components. However, 64-bit versions of Windows may recognize some 16-bit installers and automatically convert the 16-bit installer to a 32-bit installer.

More information

To run a 16-bit program or a 32-bit program that uses 16-bit processes or 16-bit components, you must install the program on a 32-bit version of Windows. To run such a program, you can install a 32-bit version of Windows in a dual-boot configuration with the 64-bit version of Windows. Then, you can restart your computer to the 32-bit version of Windows and install the 16-bit program or 32-bit program that uses 16-bit processes or 16-bit components.

> ⓘ **Note**
>
> The 32-bit version of Windows must be installed on a separate disk volume or separate physical hard disk to function correctly. If you install a 32-bit version of Windows and a 64-bit version of Windows on the same disk volume, your computer may stop responding.
>
> You should upgrade critical 32-bit programs to a 64-bit version to take full advantage of the 64-bit hardware and the 64-bit version of Windows.

Technical support for Windows x64 editions

Your hardware manufacturer provides technical support and assistance for Microsoft Windows x64 editions. Your hardware manufacturer provides support because a Windows x64 edition was included with your hardware. Your hardware manufacturer might have customized the Windows x64 edition installation with unique components. Unique components might include specific device drivers or might include optional settings to maximize the performance of the hardware. Microsoft will provide reasonable-effort assistance if you need technical help with your Windows x64 edition. However, you might have to contact your manufacturer directly. Your manufacturer is best qualified to support the software that your manufacturer installed on the hardware.

Managing the Teams Chat icon on Windows 11

Article • 09/02/2022 • 4 minutes to read

This article describes how to manage the Chat icon on Windows 11.

Applies to: Windows 11

Introduction to Teams Chat icon on Windows 11

> **Note**
>
> This article is intended for use by IT professionals who want to manage the Chat icon on Windows 11. If you're looking for more information about Chat in Windows 11, see **Get started with Chat in Windows 11**.

There are two different versions of Teams on Windows 11:

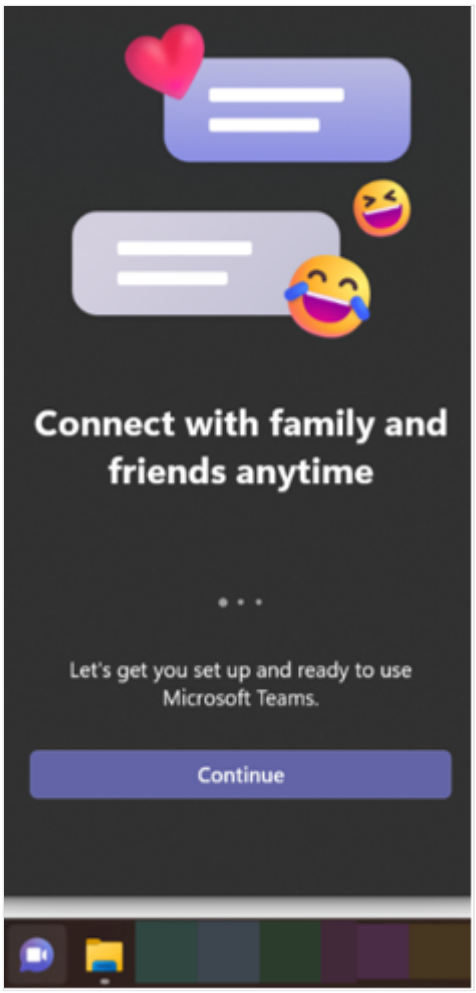
- The first is installed by default and is intended for personal use through a Microsoft account.
- The second is for an enterprise environment in which the Teams app and infrastructure will be managed by an administrator. This version is intended to be used through a work or school account.

After Windows 11 is installed, you can start using the default version of Teams Chat. By default, Chat is pinned to the taskbar, and you can use your personal account to start a call or a chat session with your colleagues or friends. To use a work or school account, you must have the Teams version installed for the work environment.

> **Note**
>
> The Teams for work app is not included in the Windows 11 installer and will not be installed until you set it up. Before you install the Teams app, there will be an app icon (small camera) on the taskbar.

Scenario 1: Chat icon is present on the Taskbar, but Teams isn't installed.

If you see the Chat icon on the Taskbar but you don't see the Teams app, select the **Chat** icon, and then check whether the following screen appears.



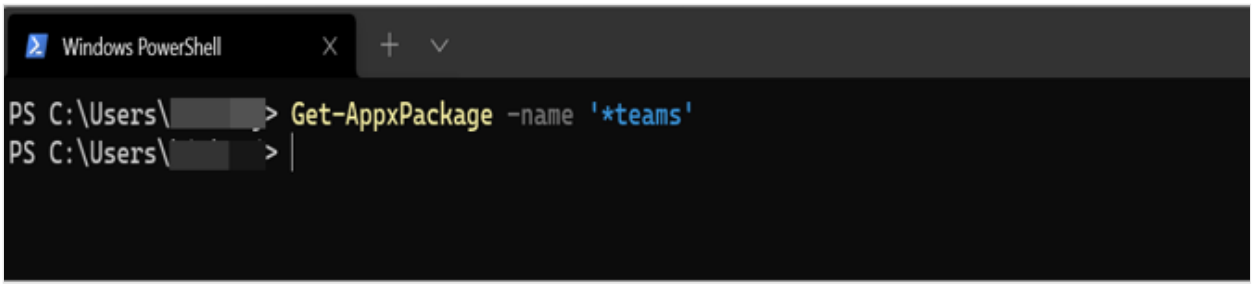
If you see this screen, select **Continue** to set up Teams.

> **Note**
>
> This indicates that Teams is not installed. Select **Continue** to proceed with installing the app for the logged-on user.

Run the following PowerShell cmdlet to check whether the Windows 11-based device has Teams installed:

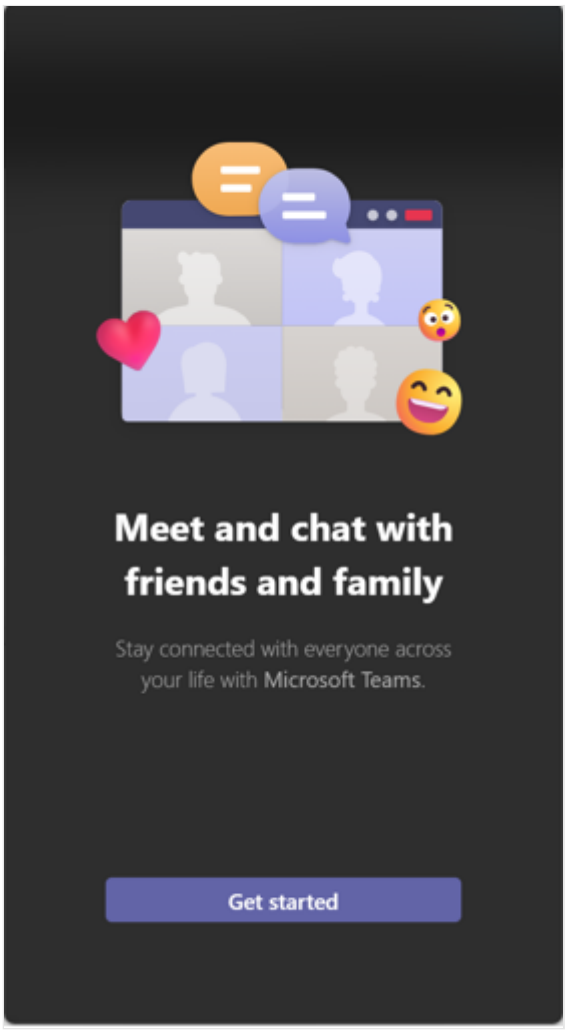
```PowerShell
Get-AppxPackage -name '*teams'
```

If this command displays no results, the Teams app isn't installed.



Scenario 2: Chat icon is turned on, but Teams isn't configured.

If you see the Chat icon on the taskbar, select the **Chat** icon, and then check whether the following screen appears.



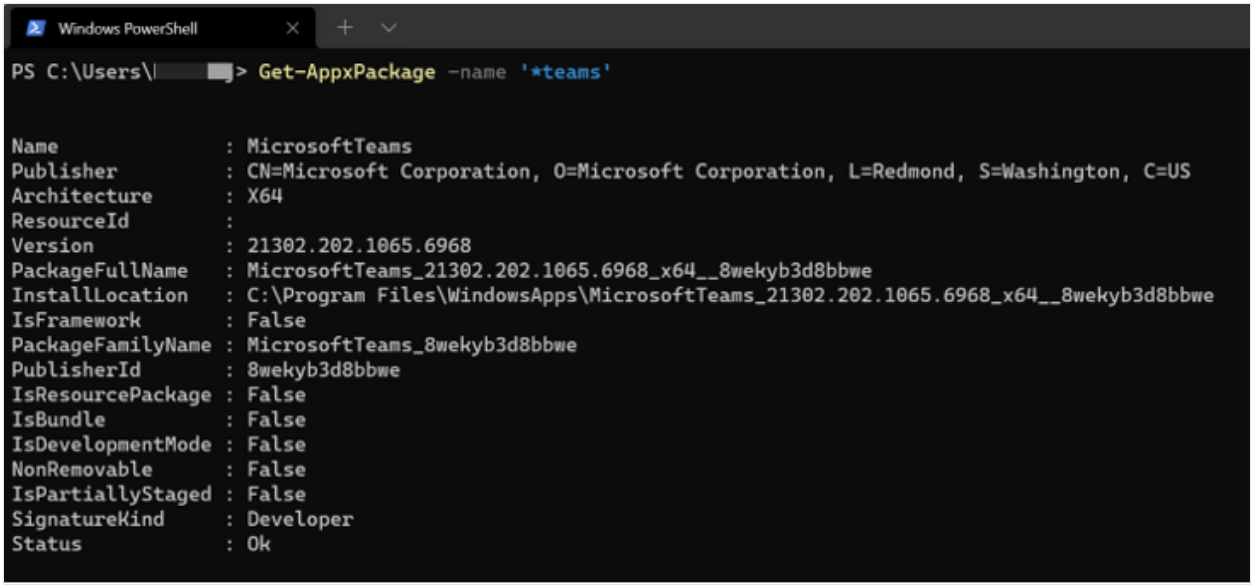
This screen indicates that Teams is installed, but not configured for the logged-on user. To configure Teams, select **Get Started**.

Alternatively, users can also run the following PowerShell cmdlet to confirm the installation status of Teams:

```
PowerShell
```

```
Get-AppxPackage -name '*teams'
```

If this command returns the installation status, the Teams app is installed.



You'll see the same results when you configure Teams. Also, you should see a list of contacts in the Chat window.

> ⓘ **Note**
>
> When you select **Get Started** and complete the configuration of Teams, a list of contacts appears in place of the Get Started screen which means that Teams is installed and fully configured.

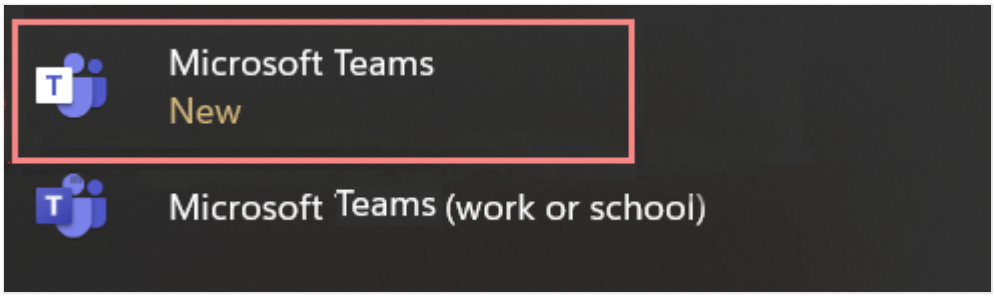
Scenario 3: Chat icon is turned off and Teams app is installed.

Admins can choose to disable the Chat icon on the taskbar. If the Teams app is installed, the app will appear on **Start** > **All apps** > **Microsoft Teams**.

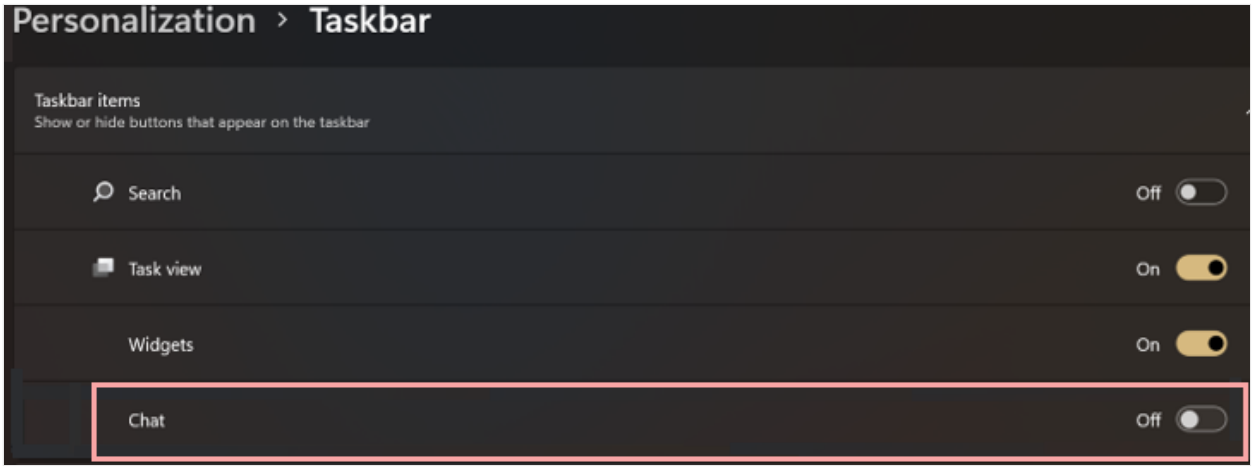
You can also verify the installation by running the following PowerShell cmdlet:

PowerShell

```
Get-AppxPackage -name '*teams'
```



To turn on Chat, right-click the taskbar, select **Taskbar settings**, and then move the Chat slider to **On**.

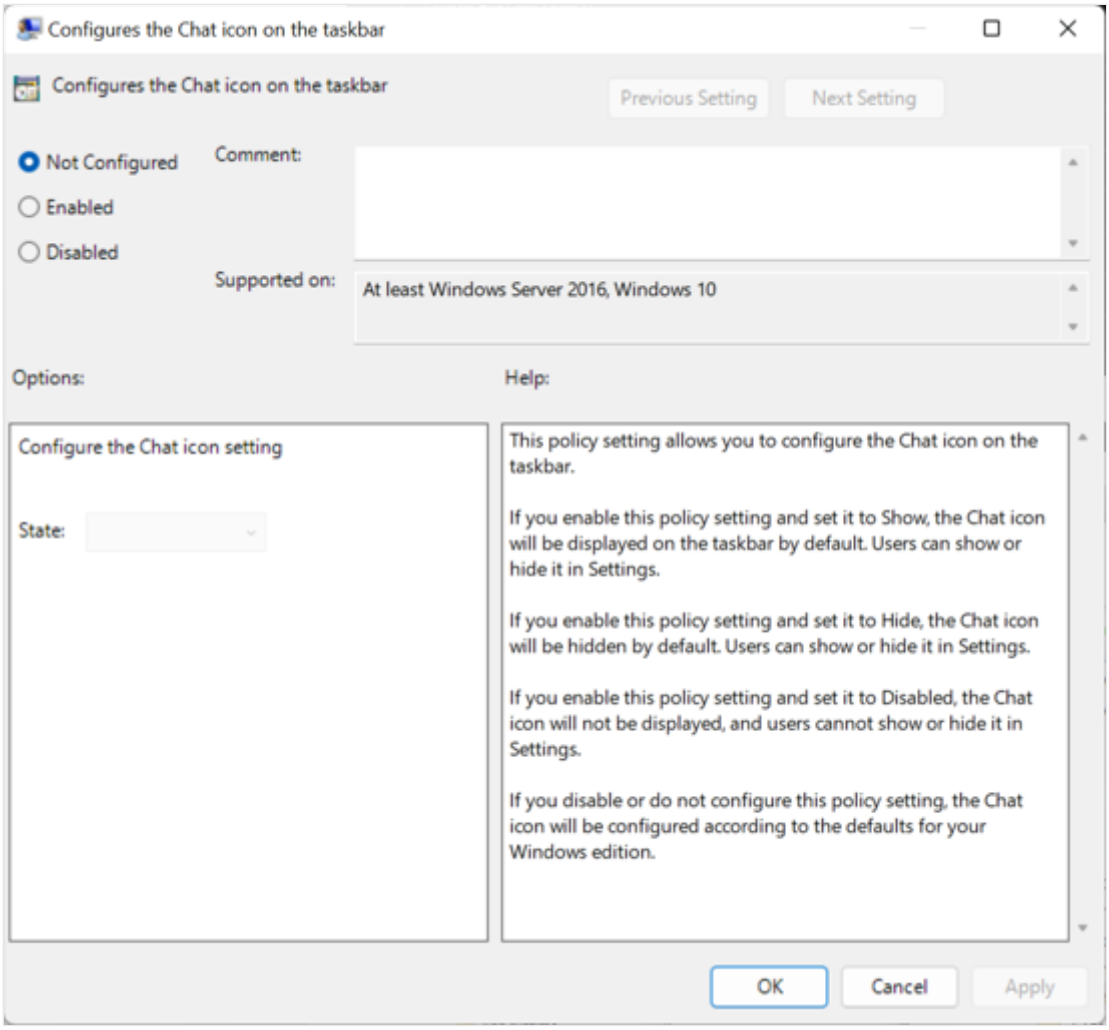


Using Group Policy settings

Admins can customize Group Policy settings, such as Show, Hide, and Disabled, for the Chat icon.

> ⓘ **Note**
>
> The **Disabled** option is available on the **Enabled** > **State list**. Do not confuse this command with setting the policy to **Disabled**. The policy is located under *Computer Configuration\Administrative Templates\Windows Components\Chat*.

You can configure the Chat icon on the taskbar using the following dialog box.



Removing the Chat icon using Intune

Use the new CSP setting, "Experience/ConfigureChatIcon", which removes the Chat icon. This requires the Enterprise or Education edition. For more information, see Policy CSP – Experience.

Create a new Configuration Profile for Windows 10 and later, type *Custom* and use the following setting:

```
OMA-URI = ". /Device/Vendor/MSFT/Policy/Config/Experience/ConfigureChatIcon"
```

The values for this policy are 0, 1, 2, and 3. This policy defaults to 0 if not enabled.

- **0 – Not Configured**: The Chat icon follows the default configuration for your Windows edition.
- **1 – Show**: The Chat icon appears on the taskbar by default. You can show or hide it in Settings.
- **2 – Hide**: The Chat icon doesn't appear by default. You can show or hide it in Settings.

- **3 – Disabled**: The Chat icon doesn't appear on the taskbar. Settings are not available to show or hide the icon.

Removing the Chat icon using Intune – Settings Catalog

To remove the Chat icon using Intune – Settings Catalog, do the following steps:

1. Create a new Configuration Policy.
2. Search for Experience.
3. Select **Configure Chat icon**.

Frequently asked questions (FAQ)

As an admin, how do I uninstall the Teams app if users have installed it?

If Teams was installed, use this PowerShell cmdlet to uninstall it:

```PowerShell
remove-appxpackage -package
"MicrosoftTeams_21302.202.1065.6968_x64__8wekyb3d8bbwe"
```

Can I remove the Teams app from the default Windows image?

The default Windows image doesn't include the Teams app.

Virtualization applications don't work together with Hyper-V, Device Guard, and Credential Guard

Article • 03/09/2022 • 2 minutes to read

Many third-party virtualization applications don't work together with Hyper-V. Affected applications include VMware Workstation and VirtualBox. These applications might not start virtual machines, or they may fall back to a slower, emulated mode.

These symptoms are introduced when the Hyper-V Hypervisor is running. Some security solutions are also dependent on the hypervisor, such as:

- Device Guard
- Credential Guard

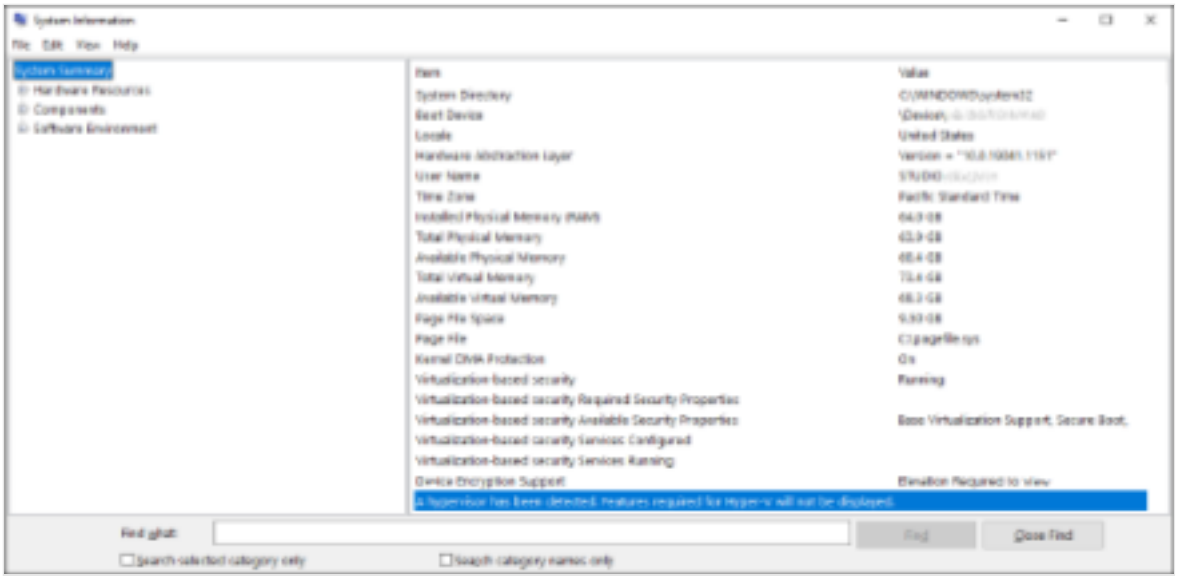
Applies to: Windows 10 - all editions
Original KB number: 3204980

Determine whether the Hyper-V hypervisor is running

To determine whether the Hyper-V hypervisor is running, follow these steps:

1. In the search box, type *msinfo32.exe*.
2. Select **System Information**.
3. In the detail window, locate the following entry:

> A hypervisor has been detected. Features required for Hyper-V will not be displayed.



Cause

This behavior occurs by design.

Many virtualization applications depend on hardware virtualization extensions that are available on most modern processors. It includes Intel VT-x and AMD-V. Only one software component can use this hardware at a time. The hardware cannot be shared between virtualization applications.

To use other virtualization software, you must disable Hyper-V Hypervisor, Device Guard, and Credential Guard. If you want to disable Hyper-V Hypervisor, follow the steps in next two sections.

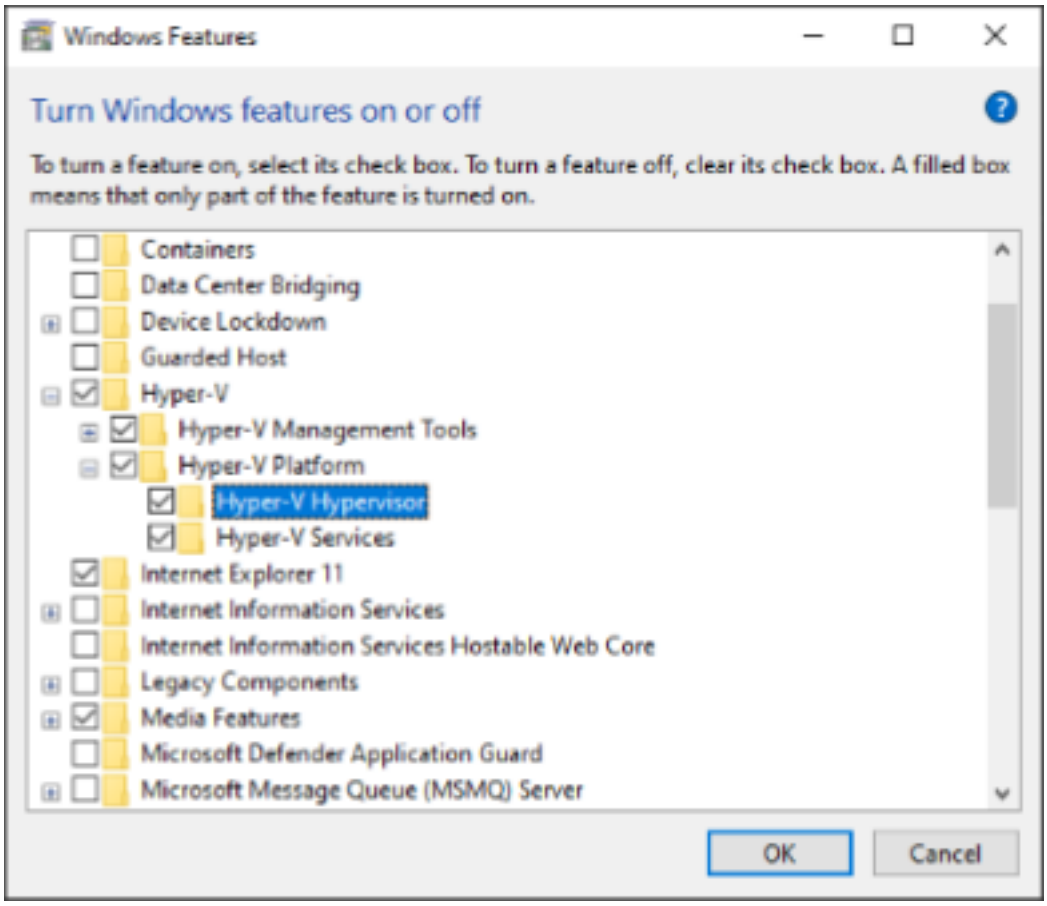
How to disable Hyper-V

You can disable Hyper-V Hypervisor either in Control Panel or by using Windows PowerShell.

Disable Hyper-V in Control Panel

To disable Hyper-V in Control Panel, follow these steps:

1. In Control Panel, select **Programs and Features**.
2. Select **Turn Windows features on or off**.
3. Expand **Hyper-V**, expand **Hyper-V Platform**, and then clear the **Hyper-V Hypervisor** check box.



Disable Hyper-V in PowerShell

To disable Hyper-V by using Windows PowerShell, follow these steps:

1. Open an elevated PowerShell window.
2. Run the following command:

```PowerShell
Disable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V-Hypervisor
```

Disable Device Guard and Credential Guard

You can disable Device Guard and Credential Guard by using registry keys or group policy. To do it, see Manage Windows Defender Credential Guard.

More information

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Register OCX and DLL files as system globals

Article • 09/23/2021 • 2 minutes to read

This article describes how to register OCX and DLL files as system globals.

Applies to: Windows 10 - all editions
Original KB number: 186597

Summary

You may receive an error when installing or running an application stating that an OCX file or a DLL file needs to be registered as system global. Make a note of the file that needs to be registered.

OCX files

1. Start your server in VGA mode.
2. You will need to use the Regsvr.exe, Regsvr16.exe (16-bit), or Regsvr32.exe (32-bit) command to register the OCX file as system global. These commands are included in the development kit when Visual Basic or Visual FoxPro is installed.

Depending on the application, you may have to register several OCX files this way.

DLL files

To register a DLL as a system global, go to the SYSTEM32 directory and locate the DLL mentioned in the error message. The command to register a file called *Sample.dll* is:

Console

```
REGISTER /S SAMPLE.DLL
```

Registration data for a program is recognized only when the program is loaded. Therefore, if you issue a `REGISTER` command for a program that is already loaded, the changes will not take effect until the next time the program is loaded.

Also note that only administrators can run `REGISTER`.

Registry key WOW6432Node may be listed in system registry in 32 bit (x86) version of Windows 7

Article • 11/26/2021 • 2 minutes to read

This article fixes an issue in which a registry subkey labeled Wow6432Node is listed in system registry on x86 machines.

Applies to: Windows 7 Service Pack 1
Original KB number: 2582176

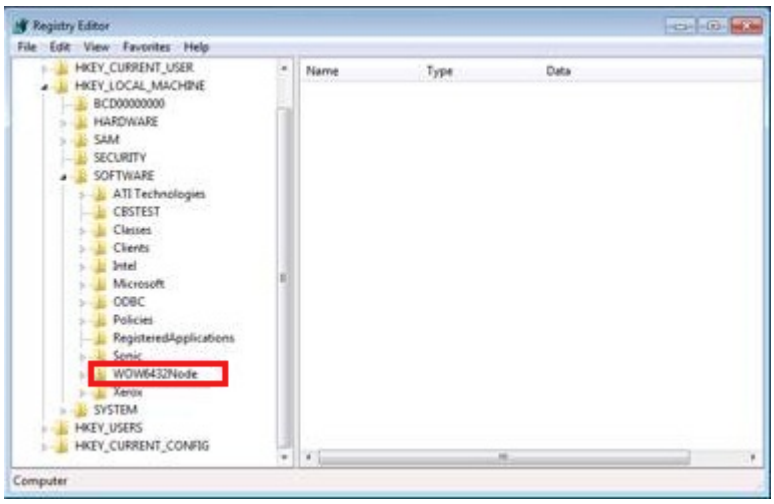
Symptoms

Consider the following scenario:

- A computer running 32 Bit (x86) Platform of Windows 7.
- Install Windows 7 with SP1 or install Windows 7 RTM Upgraded to SP1.
- Click the **Start** button, type *regedit* in the search box to open the Registry Editor.
- Expand the following registry key:

  `HKEY_LOCAL_MACHINE\SOFTWARE`

In this scenario, you may notice a registry subkey labeled **Wow6432Node** and feel that the system may have been incorrectly installed or upgraded.



Cause

This registry key is typically used for 32-bit applications on 64-bit machines. If they're present on x86 machines, they don't cause any issues as they aren't used.

Resolution

You can safely ignore the registry value.

How to determine Windows 7 platform

There are a number of tools that you can use to identify which platform is installed on the system. Below are two ways that you can use to help identify the platform

Method 1: Use System Information Tool to view Processor Architecture

1. Click on the **Start** button.
2. In the **Search** box, type the command `MSINFO32` without the quotes.
3. In the left-hand pane, click **System Summary**.
4. In the right-hand pane, view the entry labeled **System Type**.

   If the entry states **x86-Based PC**, this is 32-bit platform. If the entry states **x64-Based PC**, this is 64-bit platform.

Method 2: Use the Set command to display Processor Architecture

1. Open an Administrative command prompt
2. Type the following command:

   ```
   Console
   set processor_architecture
   ```

   If the result is **PROCESSOR_ARCHITECTURE=x86**, this is 32-bit platform. If the result is **PROCESSOR_ARCHITECTURE=AMD64** this is 64-bit platform.

References

- Registry Keys Affected by WOW64
- Registry Redirector
- 32-bit and 64-bit Application Data in the Registry

Com port settings reset to default after making changes in Device Manager

Article • 09/23/2021 • 2 minutes to read

This article describes an issue where the communications port (COM port) settings revert to the default when you restart the computer.

Applies to: Windows 2000
Original KB number: 293762

Symptoms

When you restart the computer, communications port (COM port) settings revert to the default. This issue occurs even though you've changed the settings in Device Manager. For example, if you run a command prompt in Windows 2000, you may notice that the default settings for com 1 are:

```
Baud rate=1200; Parity=None; Data Bits=7; Stop Bits=1
```

You may have a program that requires different settings, such as:

```
Baud rate=9600; Parity=None; Data Bits=8; Stop Bits=1
```

You can manually set com 1 to function at the settings you want by using this command:

```
Mode Com1: 9600,n,8,1
```

However, when you restart the system, you find that the setting reverts back to the default:

```
Baud rate=1200; Parity=None; Data Bits=7; Stop Bits=1
```

Cause

In Microsoft Windows 2000, COM port settings for command functions are maintained only for the active Windows session. Custom settings are discarded at shutdown.

Resolution

To resolve this issue, create a startup task that sets the COM port to the settings that you want. The task can be set to run minimized with the **close window on exit** setting selected.

A sample shortcut has this command line:

```
C:\winnt\system32\mode.com com1: 9600,n,8,1
```

Printer VBScript error: 0x1A8. Object required

Article • 09/23/2021 • 3 minutes to read

This article provides help to fix a 0x1A8 error that occurs when you use the print-related Visual Basic script files on a 64-bit Windows operating system.

Applies to: Windows Server 2003
Original KB number: 2466246

Symptoms

You may receive a message similar to one of the following if you attempt to use the print-related Visual Basic script files on a 64-bit Windows operating system.

- Unable to enumerate printers, error: 0x1A8. Object required
- Unable to enumerate printers on server, error: 0x1A8. Object required
- Unable to enumerate forms, error: 0x1A8. Object required
- Unable to enumerate ports, error: 0x1A8. Object required
- Unable to enumerate drivers, error: 0x1A8. Object required
- Unable to add printer connection, error: 0x1A8. Object required
- Unable to delete printer connection, error: 0x1A8. Object required
- Unable to get the default printer, error: 0x1A8. Object required
- Unable to set the default printer, error: 0x1A8. Object required
- Unable to add driver, error: 0x1A8. Object required
- Unable to delete driver, error: 0x1A8. Object required
- Unable to delete drivers on server, error: 0x1A8. Object required
- Unable to list drivers, error: 0x1A8. Object required
- Unable to print the dependent files, error: 0x1A8. Object required
- Unable to add form, error: 0x1A8. Object required
- Unable to delete form, error: 0x1A8. Object required
- Unable to delete printer, error: 0x1A8. Object required
- Unable to save the configuration of the printer, error: 0x1A8. Object required
- Unable to restore the configuration of the printer, error: 0x1A8. Object required
- Unable to get the configuration for the port, error: 0x1A8. Object required
- Unable to convert the port, error: 0x1A8. Object required
- Unable to add the TCP port, error: 0x1A8. Object required
- Unable to list ports, error: 0x1A8. Object required
- Unable to get port configuration, error: 0x1A8. Object required

- Unable to update port settings, error: 0x1A8. Object required
- Unable to get the printer config, error: 0x1A8. Object required
- Unable to configure printer, error: 0x1A8. Object required
- Unable to pause printer, error: 0x1A8. Object required
- Unable to resume printer, error: 0x1A8. Object required
- Unable to purge printer, error: 0x1A8. Object required
- Unable to send test page to printer, error: 0x1A8. Object required
- Unable to list printers, error: 0x1A8. Object required

Cause

You must register PRNADMIN.DLL with the 32-bit version of REGSVR32.EXE, and also run the script using the 32-bit version of CSCRIPT.EXE.

Resolution

- Use REGSVR32.EXE located in the %windir%\syswow64 folder to register PRNADMIN.DLL.

  Console

  ```
  %windir%\syswow64\regsvr32.exe PRNADMIN.DLL
  ```

- Use CSCRIPT.EXE located in the %windir%\syswow64 folder to run the script:

  Console

  ```
  %windir%\syswow64\cscript.exe <vbscript>
  ```

More information

The following visual basic scripts for manipulating printers are included with the Windows Server 2003 Resource Kit.

- clean.vbs - delete all printing components from the specified machine, as if the machine were clean installed.
- clone.vbs - printer server cloning script for Windows .NET Server 2003
- conall.vbs - connects to all printers on a print server
- defprn.vbs - default printer script for Windows .NET Server 2003
- drvmgr.vbs - driver script for Windows .NET Server 2003

- forms.vbs - form script for Windows .NET Server 2003
- persist.vbs - script for saving and restoring printer configuration
- portconv.vbs - Script for converting lpr ports to tcp ports
- PortMgr.vbs - Port operation script for Windows .NET Server 2003
- prncfg.vbs - printer configuration script for Windows .NET Server 2003
- prnctrl.vbs - printer control script for Windows .NET Server 2003
- prndata.vbs - printer data configuration script for Windows .NET Server 2003
- prnmgr.vbs - printer script for Windows .NET Server 2003

Resource Kit support policy

The software supplied in the Windows Resource Kit Tools is not supported under any Microsoft standard support program or service. The software (including instructions for its use and all printed and online documentation) is provided as is without warranty of any kind. Microsoft further disclaims all implied warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose. The entire risk arising out of the use or performance of the SOFTWARE and documentation remains with you.

USMT 4.0 migration from x86 to x64 results in corrupted COM+ components

Article • 09/23/2021 • 2 minutes to read

This article helps solve an issue where COM+ component settings will be corrupt when you migrate from an x86 platform to an x64 platform.

Applies to: Windows 10 – all editions
Original KB number: 2481190

Symptoms

Using the User State Migration Tool (USMT) 4.0 to migrate from an x86 platform to an x64 platform, COM+ component settings will be corrupt.

> **Note**
>
> The issue doesn't happen when migrating from x86 to x86 or x64 to x64 platforms.

Opening COMEXP.MSC or DCOMCNFG.EXE and navigating to Component Services\Computers\My Computer will result in the following on-screen error:

> You do not have permission to perform the requested action.

Additionally, you may see Event ID 4434 logged in the Application log:

> Log Name: Application
> Source: Complus
> Event ID: 4434
> Level: Warning
> User: N/A
> Task Category: Security
> Keywords: Classic
> Computer: `win7-1.contoso.com`

A method call to an object in a COM+ application was rejected because the caller isn't properly authorized to make this call. The COM+ application is configured to use Application and Component level access checks, and enforcement of these checks is currently enabled. The remainder of this message provides information about the

component method that the caller attempted to invoke and the identity of the caller.SVC/Lvl/Imp = 10/6/3, Identity=<<DOMAIN\Username>>

Cause

This is a known issue with USMT when migrating from x86 to x64.

Resolution

Workaround

To work around the issue in USMT 4.0, you must specify a config.xml file and set the "Microsoft-Windows-COM-ComPlus-Setup" to not migrate.

If you're not already using a config.xml file for USMT, you can generate one automatically by specifying the /genconfig switch to scanstate.exe syntax. For example:

scanstate.exe /genconfig:config.xml /i:migdocs.xml /i:migapp.xml

For more information about USMT and config.xml files, see the following Microsoft TechNet Article:

USMT .xml Files

Once you've generated the config.xml file, you must edit the following section, depending on source operating system (OS):

Windows XP - <component displayname=" Microsoft-Windows-COM-ComPlus-Setup-DL " migrate=" no "

Windows Vista or Windows 7 - <component displayname=" Microsoft-Windows-COM-ComPlus-Setup " migrate=" no "

Save your changes to config.xml. Include the updated config.xml when using scanstate.exe to work around the issue. For example:

scanstate.exe c:\mystore /i:migdocs.xml /i:migapp.xml /config:config.xml /v:5

This will execute scanstate.exe, using c:\mystore as the migration store, and include MigDocs.XML, MigApp.xml, and Config.XML for the migration with verbose logging enabled.

More information

If you're in a scenario in which you have already migrated and COM+ is corrupted, you can use the following procedure to restore the original COM+ repository:

From an administrative command prompt, run these three commands:

```
Console

CD %windir%\winsxs\
CD *amd64*com-complus*runtime*
Dir
```

Verify that R000000000001.clb is present. Then, copy it from the current directory to the root of the C drive by running this command:

```
Console

copy R000000000001.clb C:\R000000000001.clb
```

Next, copy, and paste the following VB script (between the dashed lines) to a.txt file and rename it COM_Restore.vbs (make sure to change the .txt file extension to .vbs).

```
Visual Basic Script


'========================================================================
=
Dim objComCatalog

Set objComCatalog = CreateObject("COMAdmin.COMAdminCatalog")
objComCatalog.RestoreREGDB "C:\R000000000001.clb"

 MsgBox "Backup Restored!"
Set objComCatalog = Nothing

'========================================================================
=
```

Save the script to the root of C:\.

From the command prompt, run this command:

```
Console

 C:\cscript COM_Restore.vbs
```

Once you see the pop-up message stating that the backup is restored, restart the computer (this is required).

Finally, open Component Servers (dcomcnfg.exe) and see if you're still getting errors.

> **Note**
>
> If you're logging in as a non-admin user and trying to start Component Services, the Event ID 4434 is expected. Non-admin users aren't part of the administrator role of the COM+ System Application and, therefore, the security warning will get logged in the event log. This doesn't mean that the COM+ catalog is corrupted.

Error when you call many objects from one process to another by using COM+: Not enough storage is available to complete this operation (0x8007000e)

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where calling many objects from one process to another by using Microsoft COM+ fails.

Applies to: Windows 10 - all editions
Original KB number: 890425

Symptoms

When you call many objects from one process to another by using Microsoft COM+, you may receive the following error message:

> Not enough storage is available to complete this operation (0x8007000e)

If you attach a debugger to the client process, you may see 8007000E first chance exceptions reported by the debugger.

Cause

This problem is caused by the limitation in the remote procedure call (RPC) layer where only 256 unique interfaces can be called from one process to another. This problem typically occurs when you use COM+ or Microsoft Transaction Server with many objects in the program or package.

Resolution

To resolve this problem, use one of the following methods:

- Split objects between multiple processes.
- Reduce the number of interfaces that are called between one process and another.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed at the beginning of this article.

DCOM event ID 10016 is logged in Windows

Article • 11/30/2021 • 2 minutes to read

This article provides a workaround to solve the event 10016 that's logged in Windows when accessing DCOM components.

Applies to: Windows 10 - all editions, Windows Server 2019, Windows Server 2016
Original KB number: 4022522

Symptoms

On a computer that's running Windows 10, Windows Server 2019, or Windows Server 2016, the following event is logged in the system event logs.

```
Source:        Microsoft-Windows-DistributedCOM
Event ID:      10016
Description: The application-specific permission settings do not grant Local
Activation permission for the COM Server application with CLSID
{D63B10C5-BB46-4990-A94F-E40B9D520160}
and APPID
{9CA88EE3-ACB7-47C8-AFC4-AB702511C276}
to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) from address LocalHost (using
LRPC) running in the application container Unavailable SID (Unavailable).
This security permission can be modified using the Component Services
administrative tool.d

Source:        Microsoft-Windows-DistributedCOM
Event ID:      10016
Description: The application-specific permission settings do not grant Local
Activation permission for the COM Server application with CLSID
{260EB9DE-5CBE-4BFF-A99A-3710AF55BF1E}
and APPID
{260EB9DE-5CBE-4BFF-A99A-3710AF55BF1E}
to the user machine\user SID (S-1-5-21-xxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx)
from address LocalHost (using LRPC) running in the application container
Microsoft.Windows.ShellExperienceHost_10.0.14393.726_neutral_neutral_cw5n1h2
txyewy SID (S-1-15-2-xxxxxxxxx-xxxxxxxxxx-xxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
xxxxxxxxxx-xxxxxxxxxx). This security permission can be modified using the
Component Services administrative tool.

Source:        Microsoft-Windows-DistributedCOM
Event ID:      10016
Description: The machine-default permission settings do not grant Local
Activation permission for the COM Server application with CLSID
```

```
{C2F03A33-21F5-47FA-B4BB-156362A2F239}
and APPID
{316CDED5-E4AE-4B15-9113-7055D84DCC97}
to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) from address LocalHost
(using LRPC) running in the application container Unavailable SID
(Unavailable). This security permission can be modified using the Component
Services administrative tool.

Source:        Microsoft-Windows-DistributedCOM
Event ID:      10016
Description: The application-specific permission settings do not grant Local
Activation permission for the COM Server application with CLSID
{6B3B8D23-FA8D-40B9-8DBD-B950333E2C52}
and APPID
{4839DDB7-58C2-48F5-8283-E1D1807D0D7D}
to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) from address LocalHost
(using LRPC) running in the application container Unavailable SID
(Unavailable). This security permission can be modified using the Component
Services administrative tool.
```

Cause

These 10016 events are recorded when Microsoft components try to access DCOM components without the required permissions. In this case, this behavior is expected and by design.

A coding pattern has been implemented where the code first tries to access the DCOM components with one set of parameters. If the first attempt is unsuccessful, it tries again with another set of parameters. The reason why it doesn't skip the first attempt is because there are scenarios where it can succeed. In those scenarios, it's preferable.

Workaround

These events can be safely ignored because they don't adversely affect functionality and are by design. It's the recommend action for these events.

If desired, advanced users and IT professionals can suppress these events from view in the Event Viewer. To do it, create a filter and manually edit the filter's XML query similar to the following one:

```

<QueryList>
  <Query Id="0" Path="System">
    <Select Path="System">*</Select>
    <Suppress Path="System">
      *[System[(EventID=10016)]]
```

```
      and
      *[EventData[
        (
          Data[@Name='param4'] and Data='{D63B10C5-BB46-4990-A94F-
E40B9D520160}' and
          Data[@Name='param5'] and Data='{9CA88EE3-ACB7-47C8-AFC4-
AB702511C276}' and
          Data[@Name='param8'] and Data='S-1-5-18'
        )
        or
        ( Data[@Name='param4'] and Data='{260EB9DE-5CBE-4BFF-A99A-
3710AF55BF1E}' and
          Data[@Name='param5'] and Data='{260EB9DE-5CBE-4BFF-A99A-
3710AF55BF1E}'
        )
        or
        (
          Data[@Name='param4'] and Data='{C2F03A33-21F5-47FA-B4BB-
156362A2F239}' and
          Data[@Name='param5'] and Data='{316CDED5-E4AE-4B15-9113-
7055D84DCC97}' and
          Data[@Name='param8'] and Data='S-1-5-19'
        )
        or
        (
          Data[@Name='param4'] and Data='{6B3B8D23-FA8D-40B9-8DBD-
B950333E2C52}' and
          Data[@Name='param5'] and Data='{4839DDB7-58C2-48F5-8283-
E1D1807D0D7D}' and
          Data[@Name='param8'] and Data='S-1-5-19'
        )
      ]]
    </Suppress>
  </Query>
</QueryList>
```

In this query:

- **param4** corresponds to the COM Server application CLSID.
- **param5** corresponds to the APPID.
- **param8** corresponds to the security context SID.

All of them are recorded in the 10016 event logs.

For more information about manually constructing Event Viewer queries, see Consuming Events.

You can also work around this issue by modifying the permissions on DCOM components to prevent this error from being logged. However, we don't recommend this method because:

- These errors don't adversely affect functionality
- Modifying the permissions can have unintended side effects.

Windows 8.1 Microsoft Store app package updates available for download

Article • 03/24/2022 • 3 minutes to read

This article outlines the release cycle for administrators to update the Microsoft Store apps installed by default on Windows 8.1-based computers.

Applies to: Windows 10 - all editions
Original KB number: 2971128

More information

When you're connected to the Internet, Windows 8.1 clients obtain updates to Microsoft Store apps directly from the Microsoft Store app. The Microsoft Store app is visible on the Windows Start screen.

To update these Microsoft Store apps on computers that can't connect to the Microsoft Store site by using the Internet, Microsoft has a collection of downloadable updates available on the Windows Update Catalog. These updates can be distributed by using System Center, WSUS, and third-party equivalents. Or, they can be slipstreamed into the operating system image that's used by your organization.

The intent of this process isn't to bypass the Microsoft Store, but to enable computers that can't connect to the Microsoft Store to update Microsoft Store apps on a recurring basis.

Frequently asked questions

Which Microsoft Store apps will be serviced through this channel

Microsoft is releasing packages for Windows 8.1 Microsoft Store apps that are listed in the release chart at the end of this article.

Will non-inbox Microsoft Store app updates be released, such as OneNote

No. We are currently targeting the Microsoft Store apps that are distributed by default with Windows 8.1 editions.

Can third-party Microsoft Store apps be updated by using this process

No. The developer of the third-party app can make available the package, and it can then be Sideload Apps with DISM similar to line-of-business apps.

Will Microsoft continue to release updates

Yes. Microsoft will update the inbox packages for Windows 8.1 for customers based on need. Contact Microsoft support to request one or more packages be updated.

How do I get the updates

These packages will be available through WSUS and the Windows Update Catalog.

Which languages are available

The packages include all the languages currently supported through the Microsoft Store.

Which editions of Windows are supported

Windows 8.1 x86 and x64 editions are supported. Windows RT 8.1 is not supported.

Can I install these updates on Industry (Embedded) editions

No, Industry editions are not licensed for these applications and therefore updates to these applications are not supported. If you have a need for Microsoft Store apps for Industry editions, contact your account manager or open a support ticket for your request to be evaluated.

How do I create an image that includes these apps

We recommend installing the app updates as part of your post operating system deployment updates through WSUS. If you need an automated process, you can extract each .cab file to its respective MSI. Then you can script the installation or deploy by using traditional application deployment technologies.

Can I use this process to reinstall the inbox apps that are removed after deploying Windows 8.1 images

No. This process is only designed to update apps already installed on the system. If you can enable temporary access to the Microsoft Store, you can install the apps again, and then maintain them by using this process. Or, you will need to deploy a new image that contains the apps.

Can the packages be installed offline

No. You can't use dism.exe to install the updates offline. They must be installed through the .MSI installer to a running operating system.

When are the packages going to be shipped

Here's the release schedule for each Microsoft Store app:

Microsoft Store App	Operating System	Release Date	Version	KB Number
Alarms	Windows 8.1	8-Jul-14	2013.1204.852.3011	2962197
BING Finance	Windows 8.1	8-Jul-14	2014.326.2159.4382	2962186
BING Food and Drink	Windows 8.1	8-Jul-14	2014.326.2200.4175	2962199
BING Health and Fitness	Windows 8.1	8-Jul-14	2014.326.2201.3773	2962187
BING Maps	Windows 8.1	8-Jul-14	2014.130.2132.1189	2962192
BING News	Windows 8.1	8-Jul-14	2014.326.2203.2627	2962188
BING Sports	Windows 8.1	8-Jul-14	2014.326.2204.2598	2962189
BING Travel	Windows 8.1	8-Jul-14	2014.326.2205.5913	2962190
BING Weather	Windows 8.1	8-Jul-14	2014.326.2207.211	2962191
Calculator	Windows 8.1	8-Jul-14	2013.1007.1950.2960	2962196
Communications Apps (People, Mail, Calendar)	Windows 8.1	24-Jun-14	2014.219.1943.3721	2962182
Help and Tips	Windows 8.1	24-Jun-14	2014.331.1818.1664	2962194
Reader	Windows 8.1	24-Jun-14	2014.312.322.1510	2962193

Microsoft Store App	Operating System	Release Date	Version	KB Number
Reading List	Windows 8.1	8-Jul-14	2013.1218.27.757	2962195
Scan	Windows 8.1	8-Jul-14	2013.1007.2015.3834	2962200
Skype	Windows 8.1	8-Jul-14	2014.402.1024.4106	2962201
Sound Recorder	Windows 8.1	8-Jul-14	2013.1010.500.2928	2962198
XBOX Games	Windows 8.1	8-Jul-14	2013.1011.10.5965	2962183
XBOX Music	Windows 8.1	8-Jul-14	2014.321.1036.1167	2962184
XBOX Video	Windows 8.1	8-Jul-14	2014.326.530.5303	2962185

Modern apps or application packages are reported as vulnerable

Article • 02/24/2022 • 2 minutes to read

This article provides resolutions for the issue in which modern apps or application packages are reported by vulnerability scanning.

Original KB number: 5011324

Some modern apps or application packages are reported as vulnerable by system vulnerability scanning, and can't be resolved by updating to the latest version.

Multiple app folders in the system

If there are multiple user profiles in the system, apps installed per users may create multiple app folders because of different versions. The folders are in the *C:\Program Files\WindowsApps* hidden folder.

Multiple app versions in the system

Consider the following scenarios:

- Several users are signed in at the same time and Microsoft Store is enabled. One user is using the app during a Microsoft Store background update.
- Some users don't sign in frequently and Microsoft Store is disabled. The system administrator updates the app manually.

In these scenarios, there are multiple versions of the app per users in the system, which doesn't affect users. However, the app or application package is reported as vulnerable if the app isn't updated for all users.

Update the app for all users or remove the old packages

To resolve this issue, use one or more of the following methods:

- Ensure that the app is updated for all users in the system.
- Remove the old packages (`.appx`) by using one of the following cmdlets:

- The Deployment Image Servicing and Management (DISM) cmdlet Remove-AppxProvisionedPackage:

  ```
  PowerShell

  Remove-AppxProvisionedPackage  -PackageName <Application Name>
  ```

- The Appx cmdlets (Get-AppxPackage and Remove-AppxPackage):

  ```
  PowerShell

  Get-AppxPackage <Application Name> -AllUsers | Remove-AppxPackage -Allusers
  ```

- Delete the user profiles pointing to the old version of the app.

To confirm that the app is updated for all users and the old packages are removed, scan again or check the *C:\Program Files\WindowsApps* folder. If you don't have the permission to check the folder, create a copy in another location and check inside.

"HRESULT: 0x80070BC9" error message while you're installing an MSI package during Windows setup or hotfix installation

Article • 09/23/2021 • 2 minutes to read

This article provides help to fix the 0x80070BC9 error that occurs when you're installing an MSI package during Windows setup or hotfix installation.

Applies to: Windows 7 Service Pack 1
Original KB number: 3024471

Symptoms

While you're installing an MSI package, you may receive an error message that resembles the following:

> Installation of assembly component {guid id} failed HRESULT: 0x80070BC9. <Ok>

If you capture an MSI log, you see the following "more information" pointer to the CBS log:

> MSI (s) (1C:38) <DateTime>: Note: 1: 1935 2: {matching guid id} 3: 0x80070BC9 4:
>
> MSI (s) (1C:38) <DateTime>: Assembly Error (sxs): Look into Component Based Servicing Log located at 1608941560ndir\logs\cbs\cbs.log to get more diagnostic information.

If you examine the CBS log, you may also see a message whose time stamp corresponds to the time of the failure:

> <DateTime>, Error CSI 00001928 (F) Impactful transactions are disabled at this time, cannot continue.[gle=0x80004005]

Note

This issue may occur under any of the following conditions:

- During certain hotfix installations
- During an installation for which someone has pre-created the installation image
- If you are incorporating an MSI installer package in an unattended installation.

Cause

As the CBS log indicates, the operating system disables transactions that may affect the system. These transactions include MSI packages that may be trying to run at this point.

Resolution

To resolve this issue, restart the system, and then run the MSI installation manually after the Setup program is complete.

More information

You may also encounter this issue when you install certain system updates or hotfixes. Typically, a restart will be required to complete the update installation. If the restart is postponed, the system tries to install MSI packages during this time, and you may encounter a situation that will prevent the MSI package installation.

After you encounter this issue, it will not be resolved unless you restart the computer and make sure that the change is applied.

Error when trying to uninstall an application: Error opening installation log file. Verify that the specified location exists and is writable

Article • 09/23/2021 • 2 minutes to read

Applies to: Windows 10 - all editions
Original KB number: 2564571

Summary

When you attempt to uninstall any product in "Programs and Features", a new "Windows Installer" window appears and gives the following error:

> Error opening installation log file. Verify that the specified location exists and is writable.

More information

This issue occurs if the following conditions are true:

- Windows Installer Logging is enabled.
- The Windows Installer engine can't properly write the uninstallation log file.

These conditions occur if the Windows Installer's application heap becomes freed and loses the information on where to store the log file. In this situation, Windows Installer attempts to write to the location *C:\Windows\System32* and addresses it as a file. Proper behavior would be to write to the following location and file name:

C:\Users\<username>\AppData\Local\Temp\MSIxxxxxx.log.

Microsoft has confirmed it to be a problem in the operating systems listed in the Applies To section of this article.

To work around this issue, stop and restart the Explorer.exe process using Task Manager.

Enable Windows Installer logging

Article • 09/23/2021 • 3 minutes to read

Windows includes a registry-activated logging service to help diagnose Windows Installer issues. This article describes how to enable this logging service.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 223300

> **Note**
>
> The registry entry in this article is valid for all Windows operating systems.

Windows Installer logging

Windows Installer can use logging to help assist in troubleshooting issues with installing software packages. This logging is enabled by adding keys and values to the registry. After the entries have been added and enabled, you can retry the problem installation and Windows Installer will track the progress and post it to the Temp folder. The new log's file name is random. However, the first letters are *Msi* and the file name has a .log extension. To locate the Temp folder, type the following line at a command prompt:

```
Console
cd %temp%
```

To enable Windows Installer logging manually, see the following section.

Enable Windows Installer logging manually

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

To enable Windows Installer logging yourself, open the registry by using Regedit.exe, and then create the following subkey and keys:

- Path: `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer`
- Type: Reg_SZ
- Value: Logging
- Data: voicewarmupx

The letters in the value field can be in any order. Each letter turns on a different logging mode. Each letter's actual function is as follows for MSI version 1.1:

- v - Verbose output
- o - Out-of-disk-space messages
- i - Status messages
- c - Initial UI parameters
- e - All error messages
- w - Non-fatal warnings
- a - Start up of actions
- r - Action-specific records
- m - Out-of-memory or fatal exit information
- u - User requests
- p - Terminal properties
- + - Append to existing file
- ! - Flush each line to the log
- x - Extra debugging information. The x flag is available only in Windows Server 2003 and later operating systems, and on the MSI redistributable version 3.0, and on later versions of the MSI redistributable.
- * - Wildcard. Log all information except the v and the x option. To include the v and the x option, specify /l*vx.

> ⓘ **Note**
>
> This change should be used only for troubleshooting and should not be left on because it will have adverse effects on system performance and disk space. Each time that you use the **Add or Remove Programs** item in **Control Panel**, a new Msi*.log file is created. To disable the logging, remove the **Logging** registry value.

Enable Windows Installer logging with Group Policies

You can enable logging with Group Policies by editing the appropriate OU or Directory Group Policy. Under **Group Policy**, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and then select **Windows Installer**.

Double-click **Logging**, and then click **Enabled**. In the **Logging** box, enter the options you want to log. The log file, Msi.log, appears in the Temp folder of the system volume.

For more information about MSI logging, see Windows Help. To do this, search by using the phrase *msi logging*, and then select **Managing options for computers through Group Policy**.

> ⓘ **Note**
>
> The addition of the x flag is available natively in Windows Server 2003 and later operating systems, on the MSI redistributable version 3.0, and on later versions of the MSI redistributable.

Add/Remove Programs tool displays installed programs incorrectly

Article • 09/23/2021 • 5 minutes to read

This article provides a solution to an issue where the **Add/Remove Programs** tool in Control Panel displays installed programs incorrectly.

Applies to: Windows XP
Original KB number: 266668

Symptoms

When you install and uninstall programs, the Add/Remove Programs tool in Control Panel may display the installed programs incorrectly. The **Currently installed programs** box may contain only a single text string, or may display a large blank space before the program entries. Other display problems may include that there are no listed programs. Additionally, one of the following error messages may appear:

Message 1

> An unexpected error occurred. Class not registered
> res://appwiz.cpl/listbox.htc
> Line: 225

Message 2

> Object doesn't support this property or method res://appwiz.cpl/default.hta
> Line: 75

Cause

This problem may occur if the uninstaller for a program incorrectly removes registry entries that are used by Windows and the Add/Remove Programs tool.

Resolution

ⓘ Important

> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

To resolve this problem, follow these steps:

1. Click **Start**, click **Run**, and then type *CMD*.
2. At the prompt, type `REGSVR32 APPWIZ.CPL`.
3. If this fails, look for the registry entries that are listed below. To resolve this issue, check the registry for the following keys and values. Re-create any missing keys or values. These keys use the system drive letter. You may have to adjust these entries to match the configuration of your computer.

    - [HKEY_CLASSES_ROOT\CLSID{00000535-0000-0010-8000-00AA006D2EA4}] "ADODB.Recordset"
    - [HKEY_CLASSES_ROOT\CLSID{00000535-0000-0010-8000-00AA006D2EA4}\InprocServer32] "C:\Program Files\Common Files\System\ado\msado15.dll"
    - [HKEY_CLASSES_ROOT\CLSID{00000535-0000-0010-8000-00AA006D2EA4}\InprocServer32] "ThreadingModel"="Apartment"
    - [HKEY_CLASSES_ROOT\CLSID{00000535-0000-0010-8000-00AA006D2EA4}\ProgID] "ADODB.Recordset.2.5"
    - [HKEY_CLASSES_ROOT\CLSID{00000535-0000-0010-8000-00AA006D2EA4}\VersionIndependentProgID] "ADODB.Recordset"
    - HKEY_CLASSES_ROOT\CLSID{2048EEE6-7FA2-11D0-9E6A-00A0C9138C29 } "Microsoft OLE DB Row Position Library"
    - HKEY_CLASSES_ROOT\CLSID{2048EEE6-7FA2-11D0-9E6A-00A0C9138C29}\InprocServer32 "C:\Program Files\Common Files\System\Ole DB\oledb32.dll" "ThreadingModel"="Both"
    - HKEY_CLASSES_ROOT\CLSID{2048EEE6-7FA2-11D0-9E6A-00A0C9138C29}\ProgID "RowPosition.RowPosition.1"
    - HKEY_CLASSES_ROOT\CLSID{2048EEE6-7FA2-11D0-9E6A-00A0C9138C29}\VersionIndependentProgID "RowPosition.RowPosition"
    - [HKEY_CLASSES_ROOT\CLSID{352EC2B7-8B9A-11D1-B8AE-006008059382}\InProcServer32] %SystemRoot%\System32\appwiz.cpl

4. Follow the steps in one of the following procedures, as it applies to your computer, and then test to determine if this issue is resolved. If the issue is resolved, skip the remaining steps. If the issue is not resolved, go to step 5.

    - To resolve this issue with Internet Explorer 6.0 installed, repair Internet Explorer 6.0:

        a. Click **Start**, and then click **Run**.

        b. Paste the following command in the **Open** box, and then click **OK**:

        ```
        Console

        rundll32 setupwbv.dll, IE6Maintenance C:\Program Files\Internet
        Explorer\Setup\SETUP.EXE /g C:\WINDOWS\IE Uninstall Log.Txt
        ```

        Because this command is case-sensitive, Microsoft recommends that you copy the command from this article, and then paste the command in the Open box.

    - To resolve this issue with Internet Explorer 5.0 or 5.5 installed, repair Internet Explorer 5.0 or 5.5:

        a. Click **Start**, and then click **Run**.

        b. Paste the following command in the **Open** box, and then click **OK**:

        ```
        Console

        rundll32 setupwbv.dll, IE5Maintenance C:\Program Files\Internet
        Explorer\Setup\SETUP.EXE /g C:\WINDOWS\IE Uninstall Log.Txt
        ```

        Because this command is case-sensitive, Microsoft recommends that you copy the command from this article, and then paste the command in the Open box.

5. Perform an in-place upgrade:

    > **Note**
    >
    > Before you perform an in-place upgrade, make sure that you back up your data. For more information about the risks of performing an in-place upgrade, see the More Information section.

    a. Run Winnt32.exe from the \I386 directory.

b. When the Setup screen appears, proceed the upgrading.
c. Allow installation to complete.

If the Add/Remove Programs tool still does not function properly, shows no content, or if you want to try to fix this issue without upgrading to later versions of Internet Explorer, check the following registry keys to make sure that they contain entries:

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Management\ARPCache`

> **Note**
>
> If the previous registry keys are blank, the Add/Remove Programs tool may also be blank.

Use the command-line REGSVR32 [path\filename] to register each of the following files:

- %systemroot%\System32\Appwiz.cpl
- %systemroot%\System32\Mshtml.dll
- %systemroot%\System32\Jscript.dll
- %systemroot%\System32\Msi.dll
- Program Files\Common Files\System\Ole DB\Oledb32.dll
- Program Files\Common Files\System\Ado\Msado15.dll
- %systemroot%\System32\Msdart32.dll [not registerable]
- %systemroot%\System32\Mshtmled.dll
- %systemroot%\System32\Mswstr10.dll [not registerable]

If the Add/Remove Programs tool displays incomplete information or is blank, verify the file dates. Where possible, register the following files:

- %systemroot%\System32\Gdi32.dll [not registerable]
- %systemroot%\System32\User32.dll [not registerable]
- %systemroot%\System32\Msvcrt.dll [not registerable]
- %systemroot%\System32\Ole32.dll
- %systemroot%\System32\Shlwapi.dll [not registerable]
- %systemroot%\System32\Imm32.dll [not registerable]
- %systemroot%\System32\Indicdll.dll [not registerable]
- %systemroot%\System32\Urlmon.dll
- %systemroot%\System32\Version.dll [not registerable]
- %systemroot%\System32\Lz32.dll [not registerable]
- %systemroot%\System32\Comctl32.dll [not registerable]

- %systemroot%\System32\Clbcatq.dll
- %systemroot%\System32\Oleaut32.dll
- %systemroot%\System32\Mlang.dll
- %systemroot%\System32\Shell32.dll
- %systemroot%\System32\Shdoclc.dll [not registerable]
- %systemroot%\System32\NetapI32.dll [not registerable]
- %systemroot%\System32\Secur32.dll [not registerable]
- %systemroot%\System32\Netrap.dll [not registerable]
- %systemroot%\System32\Samlib.dll [not registerable]
- %systemroot%\System32\Ws2_32.dll [not registerable]
- %systemroot%\System32\Ws2help.dll [not registerable]
- %systemroot%\System32\Wldap32.dll [not registerable]
- %systemroot%\System32\Dnsapi.dll [not registerable]
- %systemroot%\System32\Wsock32.dll [not registerable]
- %systemroot%\System32\Plugin.ocx
- %systemroot%\System32\Wininet.dll [not registerable]
- %systemroot%\System32\Crypt32.dll [not registerable]
- %systemroot%\System32\Msasn1.dll [not registerable]
- %systemroot%\System32\Msls31.dll [not registerable]
- %systemroot%\System32\Imgutil.dll
- %systemroot%\System32\Cscui.dll
- %systemroot%\System32\Cscdll.dll [not registerable]

If the Add/Remove Programs tool can draw the dialog user interface, but does not display any installed program contents, check the registry for the presence of the following key:

`HKEY_CLASSES_ROOT\CLSID\{352EC2B7-8B9A-11D1-B8AE-006008059382}\InProcServer32`

If this registry key is missing, copy the following text to a text file, save the file with a .reg extension, and then double-click the file on the affected computer to return the proper entries.

For Windows Registry Editor Version 5.00:

> [HKEY_CLASSES_ROOT\CLSID{352EC2B7-8B9A-11D1-B8AE-006008059382}\InProcServer32]
> @=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,00,74,00,25,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,61,00,70,00,70,00,77,00,69,00,7a,00,2e,00,63,00,70,00,6c,00,00,00
> "ThreadingModel=Apartment"

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the Applies to section.

The following list includes all the registry keys that are used by Add/Remove Programs. These keys must be set by registering Appwiz.cpl, but they are provided here for cross-reference to confirm that the registration completed successfully.

- [HKEY_CLASSES_ROOT\CLSID{352EC2B7-8B9A-11D1-B8AE-006008059382}]

  @="%DESC_ShellAppMgr%"

- [HKEY_CLASSES_ROOT\CLSID{352EC2B7-8B9A-11D1-B8AE-006008059382}\InProcServer32]

  @="SystemRoot%\System32\appwiz.cpl"
  (REG_EXPAND_SZ)"ThreadingModel"="Apartment"

- [HKEY_CLASSES_ROOT\CLSID{0B124F8C-91F0-11D1-B8B5-006008059382}]

  @="Installed Apps Enumerator"

- [HKEY_CLASSES_ROOT\CLSID{CFCCC7A0-A282-11D1-9082-006008059382}]

  @="Darwin App Publisher"

- [HKEY_CLASSES_ROOT\CLSID{CFCCC7A0-A282-11D1-9082-006008059382}\InProcServer32]

  @="SystemRoot%\System32\appwiz.cpl"
  (REG_EXPAND_SZ)"ThreadingModel"=Apartment"

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved]

  "{352EC2B7-8B9A-11D1-B8AE-006008059382}"="Shell Application Manager"

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Management\Publishers\Darwin App Publisher] @="{CFCCC7A0-A282-11D1-9082-006008059382}"

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Approved] "{CFCCC7A0-A282-11D1-9082-006008059382}"="Darwin App Publisher"

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\InProcCPLs] "appwiz.cpl"=""

Registry entries that are used once ARP is running

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\AppInstallPath`

  Reads INF file. Code reads INF file name. INF section used is AppInstallList

- `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer\Terminal Server\EnableAdminRemote`

  Set to 1 while ARP is running. Tells TS that ARP is running. Set to 0 when ARP exits.

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Management\Publishers` Enumerates app publishers

- `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Wx86\cmdline`

  Reads to determine if wx86 is enabled.

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\NewShortcutHandlers`

  Enumerated to obtain list of new-link handlers. It looks like these handlers may add a link for a given item - for instance, to the Start menu, desktop, or other items.

- `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Shutdown\ForceReboot`

  Read to determine if a restart is required after running setup. Presence of value means must-reboot == true.

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\MS-DOSOptions`

VersionNT value for Windows 10, Windows Server 2016, and Windows Server 2019

Article • 09/23/2021 • 2 minutes to read

This article describes the VersionNT value for Windows 10, Windows Server 2016, and Windows Server 2019.

Applies to: Windows 10 - all editions, Windows Server 2019, Windows Server 2016
Original KB number: 3202260

Summary

When you install a .msi installation package in Windows 10, Windows Server 2016 or Windows Server 2019, the VersionNT value is 603.

More information

This version numbering is by design. To maintain compatibility, the VersionNT value is 603 for Windows 10, Windows Server 2016, and Windows Server 2019.

You cannot link TextService in Eudcedit.exe

Article • 12/06/2021 • 2 minutes to read

This article helps to resolve an issue in which you cannot link TextService in Eudcedit.exe.

Applies to: Windows 10, version 2004
Original KB number: 4568315

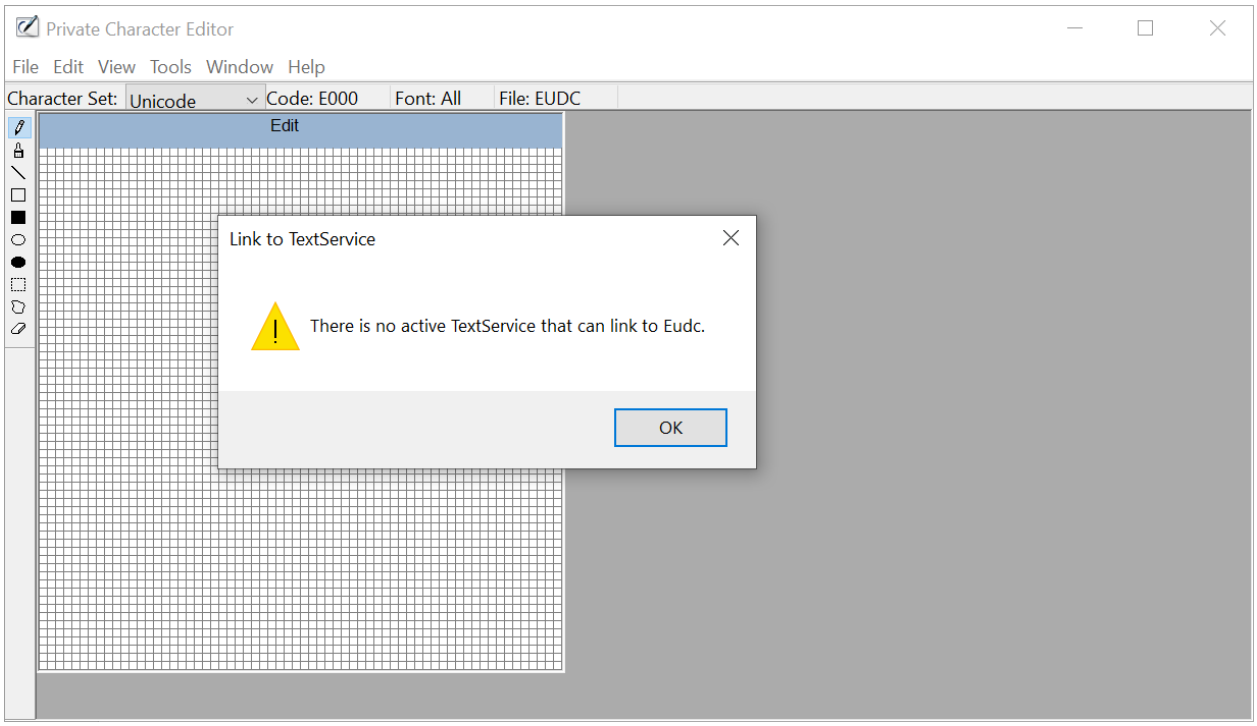
Symptoms

Consider the following scenario:

- You use Windows 10, version 2004.
- You create or modify end-user-defined characters (EUDC) on the computer.
- You try to link the EUDC to Microsoft Bopomofo.

In this scenario, the EUDC editor returns the following message:

> There is no active TextService that can link to Eudc.



Cause

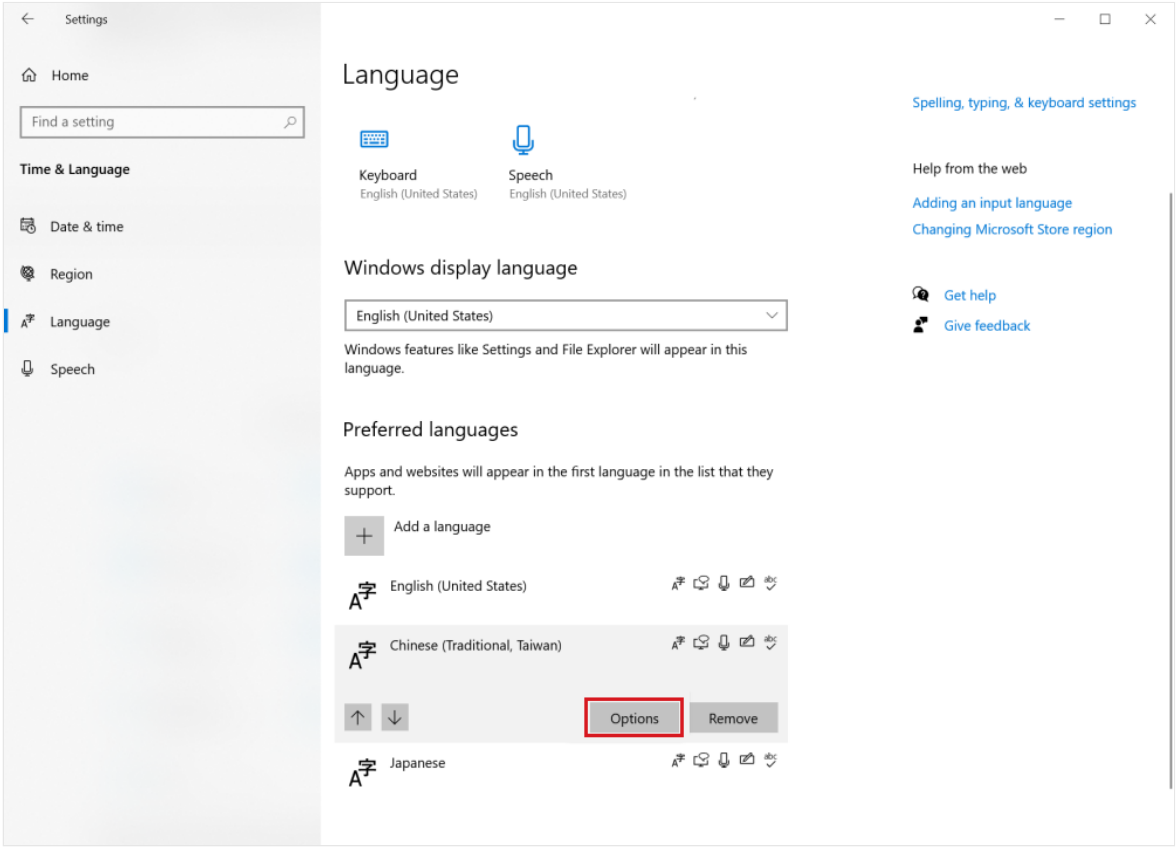
After you update to Windows 10, version 2004, Microsoft Bopomofo is updated. The latest version of Microsoft Bopomofo currently doesn't provide the functionality to link EUDC characters.

Workaround

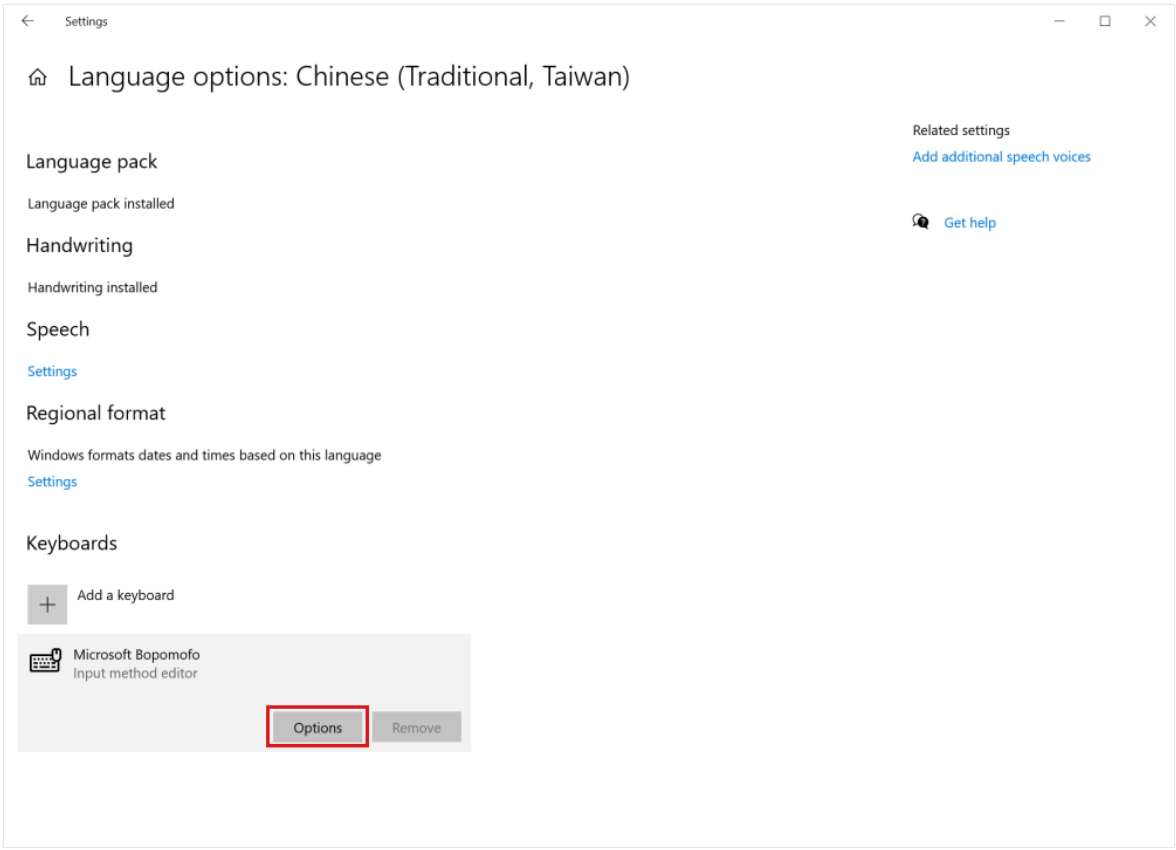
Method 1

Turn on the Compatibility option to revert to the previous version Microsoft Bopomofo. To do this, follow these steps:

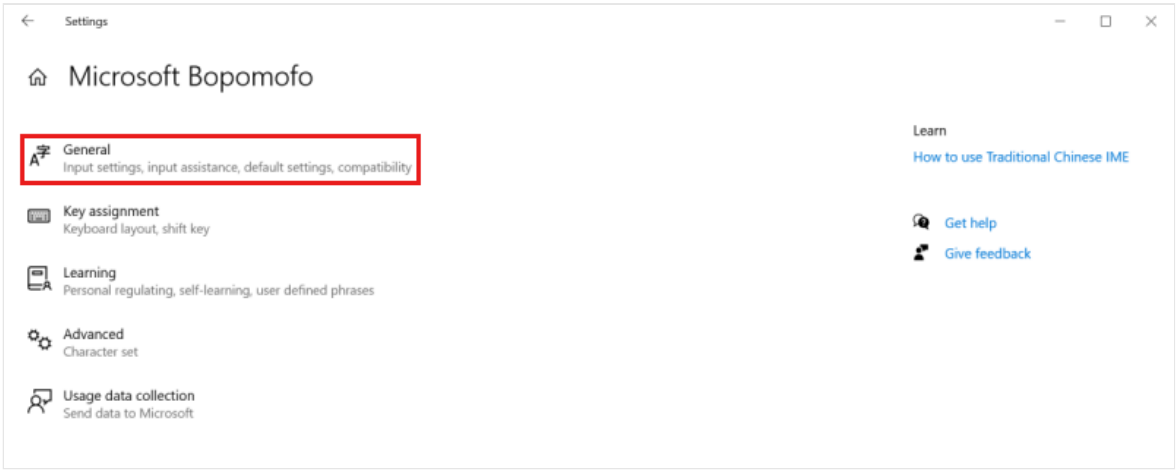
1. On the **Settings** page, select **Language**.



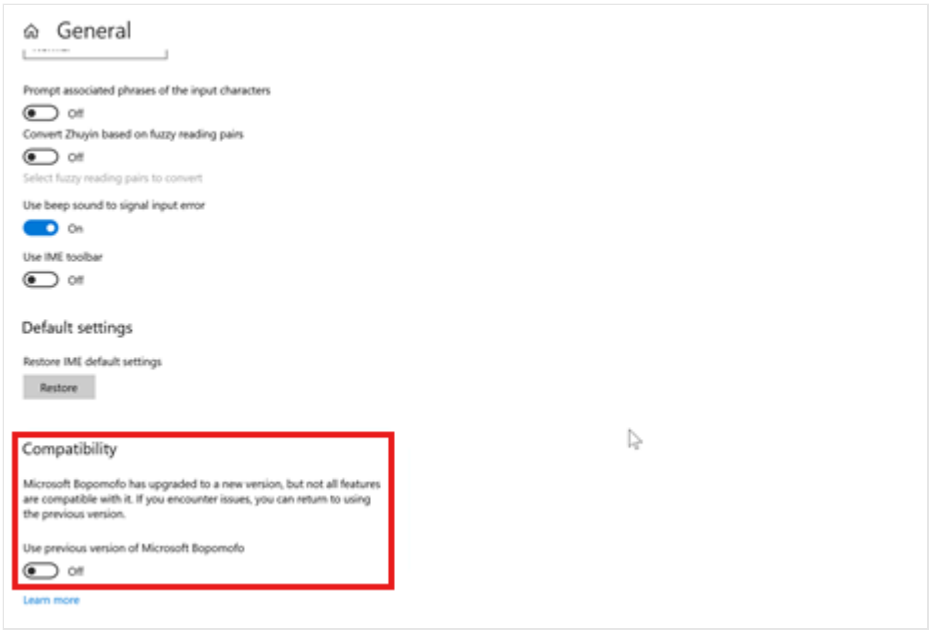
2. Select **Options** for Microsoft Bopomofo (**Chinese (Traditional, Taiwan)**).



3. Select **General**.



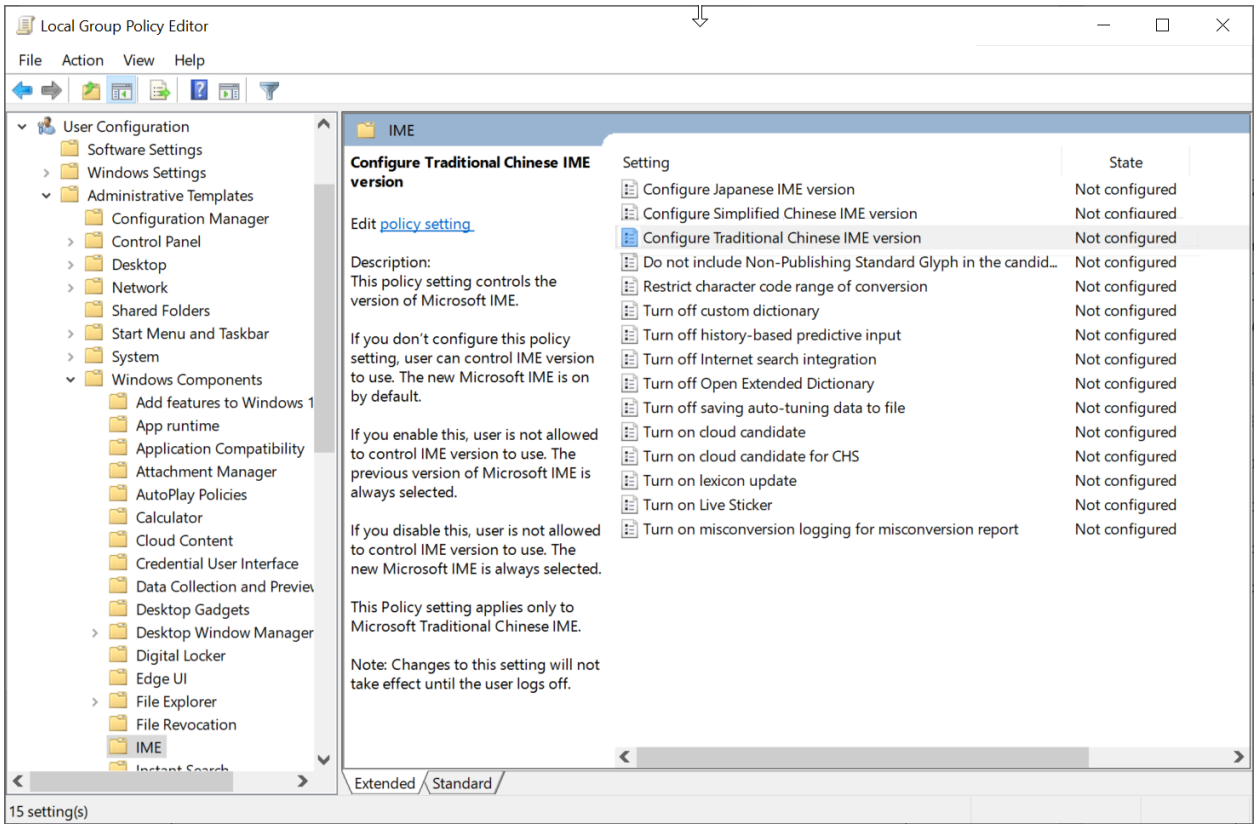
4. Turn on the "Use previous version of Microsoft Bopomofo" option.



Method 2

Revert to the previous version of Microsoft Bopomofo by using the following Group Policy setting:

User Configuration > Administrative Templates > Windows Components > IME > Configure Traditional Chinese IME version



> **Note**
>
> This policy was introduced in Windows 10, version 2004.

Method 3

Revert to the previous version of Microsoft Bopomofo by using MDM Policy. To do this, see TextInput/ConfigureTraditionalChineseIMEVersion.

How to change registry values or permissions from a command line or a script

Article • 09/23/2021 • 2 minutes to read

This article describes how to change registry values or permissions from a command line or a script.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 264584

Summary

To change a registry value or registry permissions from a command line or from a script, use the Regini.exe utility. The Regini.exe utility is included in the Windows NT Server 4.0 Resource Kit, in the Microsoft Windows 2000 Resource Kit, and in the Microsoft Windows Server 2003 Resource Kit.

> **Note**
>
> The Regini.exe utility for Windows 2000 is no longer supported and isn't available for download from Microsoft. This tool is available on the original Microsoft Windows 2000 Resource Kit CD-ROM only.

More information

The syntax for changing registry values or permissions with Regini is:
REGINI [-m *machinename*] *files*

Here, the `-m \\machinename` option is used to modify the registry of a remote machine, and *files* represents the names of the script files that contain the changes to the registry.

The text file or files should contain the registry changes in the following format.
\Registry\Hiveroot\Subkeys registry value=data [permissions]

The Regini utility works with kernel registry strings. When you gain access to the registry in User mode with `HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER`, and so on, the string is converted in Kernel mode as follows:

- HKEY_LOCAL_MACHINE is converted to `\registry\machine`.
- HKEY_USERS is converted to `\registry\user`.
- HKEY_CURRENT_USER is converted to `\registry\user\user_sid`, where user_sid is the Security ID associated with the user.
- HKEY_CLASSES_ROOT is converted to `\registry\machine\software\classes`.

For example, a script file to change the registry value `DiskSpaceThreshold` located in the HKEY_LOCAL_MACHINE hive to the value 0x00000000 would be written as follows.

Console

```
\registry\machine\system\currentcontrolset\services\lanmanserver\parameters
DiskSpaceThreshold = REG_DWORD 0x00000000
```

Registry key permissions are specified by binary numbers separated by spaces, corresponding to Regini.doc file numbers that specify certain permissions given to specific groups. (For example, the number 1 specifies Administrators - Full Control). You can use the Resource Kit utility REGDMP to get the current permissions of a registry key in the binary number format.

> **⊗ Caution**
>
> When you use Regini to change permissions, the current permissions are replaced, not edited.

The following example script file shows the syntax for changing permissions on a registry key.

Console

```
\Registry\Machine\Software [1 5 10]
```

This script modifies `HKEY_LOCAL_MACHINE\Software` to have the permissions.

Console

```
Administrators - Full Control
Creator/Owner - Full Control
Everyone - Read
```

In Windows XP and in Windows Server 2003, you must enclose the value in quotation marks. For example, you could use the following script to call AUoptions.txt.

Console

```
regini.exe -m \\remoteworkstation auoptions.txt
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\A
uto Update "ConfigVer"= REG_DWORD 1 "AUOptions"= REG_DWORD 4
"ScheduledInstallDay"= REG_DWORD 0 "ScheduledInstallTime"= REG_DWORD 1
```

For more information, see the Regini.doc file that is included in the resource kit for your specific operation system.

Application Virtualization (App-V) troubleshooting documentation

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve App-V-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

App-V sub categories

- Administration
- Application does not load or run
- Installation and configuration
- Management Server issues
- Package conversion
- Publishing server issue

How to launch processes inside the App-V 5.0 virtualized environment

Article • 09/29/2021 • 3 minutes to read

This article describes how to launch processes inside the Microsoft Application Virtualization 5.0 client (App-V 5.0) virtualized environment.

Applies to: Windows 7 Service Pack 1
Original KB number: 2848278

Summary

A common troubleshooting task for the App-V 5.0 is to investigate or modify a local package by opening a process inside the context of an App-V application. This is also known as opening a process "in the App-V bubble". App-V 5.0 offers several alternative methods to perform this task that differ significantly from techniques available in previous versions of the product. Each method detailed below accomplishes essentially the same task, but some methods may be better suited for some applications than others depending on whether the virtualized application is already running.

PowerShell cmdlet: Get-AppvClientPackage

You can use the `Start-AppVVirtualProcess` cmdlet to retrieve the package name and then start a process within the specified package's virtual environment (substitute the name of your package for <Package>):

PowerShell

```
$AppVName = Get-AppvClientPackage <Package>
Start-AppvVirtualProcess -AppvClientObject $AppVName cmd.exe
```

If you do not know the exact name of your package, you can use the command line `Get-AppvClientPackage executable`, substituting the name of the application for "executable"; for example: `Get-AppvClientPackage Word`.

This method allows you launch any command within the context of an App-V package whether the package is currently running or not. This is similar to using the `sfttray /exe cmd.exe /launch "App-V Application"` syntax in App-V 4.6.

The command-line switch "/appvpid:<PID>"

This allows you to apply the `/appvpid` switch to any command that will allow the command to run within the virtual process of the virtual process you selected by its PID (Process ID) as in the example below:

```
Console

cmd.exe /appvpid:8108
```

To obtain the process ID (PID) of your App-V process, use the command tasklist.exe from an elevated command prompt and obtain the PID of your process. This method has the advantage of launching the new executable in the same App-V environment as an already-running executable.

The command-line hook switch "/appvve:<GUID>"

Where the `/appvpid` switch requires the virtual process to already be running, this switch allows you to start a local command and allow it to run within the virtual environment of an App-V package and will initialize it. The syntax is `cmd.exe /appvve:<PACKAGEGUID_VERSIONGUID>`.

For example:

```
Console

cmd.exe /appvve: aaaaaaaa-bbbb-cccc-dddd-eeeeeeee_11111111-2222-3333-4444-
55555555
```

To obtain the package GUID and version GUID, of your application, run the `Get-AppvClientPackage` cmdlet, then concatenate the package GUID and version GUIDs with an underscore between them. For example:

```
PowerShell

PS C:\> Get-AppvClientPackage
```

Output:

> PackageId: aaaaaaaa-bbbb-cccc-dddd-eeeeeeee
> VersionId: 11111111-2222-3333-4444-55555555
> Name: MyApp 1.10

The output would yield the command line: `cmd.exe /appvve:aaaaaaaa-bbbb-cccc-dddd-eeeeeeee_11111111-2222-3333-4444-55555555`.

The Run Virtual feature

If you are working within RDS environments, and have a package that is published globally, you can also take advantage of the "Run Virtual" feature. To do this, the add process executable names as subkeys of the following key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppV\Client\RunVirtual`

For example, if you have a locally installed application named MyApp.exe and would like this application to run within the virtual environment, create a subkey called MyApp.exe. Edit the (Default) REG_SZ value that contains the package GUID and the version GUID separated by an underscore (for example, <GUID>_<GUID>).

For example, the application listed in the previous example would yield a registry export (.reg file) like the following:

registry

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppV\Client\RunVirtual]
@=""
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppV\Client\RunVirtual\MyApp.exe]
@="aaaaaaaa-bbbb-cccc-dddd-eeeeeeee_11111111-2222-3333-4444-55555555"
```

Each native process that needs to run locally will require its own subkey beneath the Run Virtual key. As long as there is one version of the EXE on the system, placing the package\version GUID combination in the default key value will suffice.

You may also specify the AppConnectionGroupID and VersionID of a globally published connection group in a similar format. Specify the main executable name in the connection group. For example, if your Connection Group XML looked like the following:

XML

```
<?xml version="1.0" ?>
<appv:AppConnectionGroup
```

```
xmlns="http://schemas.microsoft.com/appv/2010/virtualapplicationconnectiongr
oup"
xmlns:appv="http://schemas.microsoft.com/appv/2010/virtualapplicationconnect
iongroup" AppConnectionGroupId="CCCCCCCC-CCCC-CCCC-CCCC-CCCCCCCCCC"
VersionId="33333333-3333-3333-3333-3333333333" Priority="0"
DisplayName="MyApp Connection Group">
```

then you would add a registry key like this:

registry

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppV\Client\RunVirtual]
@=""
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppV\Client\RunVirtual\MyApp.exe]
@="aaaaaaaa-bbbb-cccc-dddd-eeeeeeee_11111111-2222-3333-4444-555555555
```

An App-V v5 virtualized application fails to start with error 0xc0000142

Article • 09/29/2021 • 2 minutes to read

This article provides a solution to the issue a Microsoft Application Virtualization version 5 (App-V) virtualized application fails to start with an application error 0xc0000142.

Applies to: Windows 10 - all editions
Original KB number: 2777003

Symptoms

The error appears as a popup message stating:

> The application was unable to start correctly (0xc0000142). Click OK to close the application.

You also see a related App-V Event for this application launch failure:

> Log Name: Microsoft-AppV-Client/Virtual Applications
> Source: Microsoft-AppV-Client
> Date:
> Event ID: 18005
> Task Category: Application Launch
> Level: Error
> Keywords: Virtual Application Launch
> User: contoso\user1
> Computer: TEST-PC
> Description:
> The virtual application 'path to virtualized executable' could not be started because the App-V Subsystem 'Virtual Filesystem' could not be initialized. {error: 0x74300C0A-0x20006}

Cause

This can occur if an NTFS setting called 8.3 Short name creation is disabled on the machine. This setting is governed by the value data of this registry key: `KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation`.

Resolution

You need to enable NTFS 8.3 Short name functionality on the client. To do this set the value of `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation` to 2 and reboot the machine. For more information on enabling and disabling NTFS 8.3 Short names, see How to disable 8.3 file name creation on NTFS partitions

> **Note**
>
> If the package was added to the client when Short names were disabled, you might need to remove the package using the PowerShell command Remove-AppvClientPackage and re-add the package using the method it was added initially. In addition to this, you might also need to remove the user specific information about the package. To do this, delete %LOCALAPPDATA%\Microsoft\AppV\Client\VFS\<PackageID>.
>
> If Short names were disabled on the Sequencer, but enabled on the clients, the Package should be unpublished, re-sequenced after enabling Short names on the Sequencer, and then re-published to the clients.

More Information

For more information about NtfsDisable8dot3NameCreation, see NtfsDisable8dot3NameCreation.

Current list of App-V 5.x file versions

Article • 03/24/2022 • 2 minutes to read

This article provides current list of App-V 5.x file versions.

Applies to: Windows 10 - all editions
Original KB number: 2940578

Summary

This article provides a quick reference to determine Microsoft Application Virtualization (App-V) 5.x file versions. This is helpful for support personnel in determining whether an environment is using the latest binaries.

More information

To identify the build number of the App-V client, go to the **Programs and Features** item in **Control Panel**, and then click one of the following items, as appropriate:

- Microsoft Application Virtualization (App-V) Client 5.X
- Microsoft Application Virtualization (App-V) Client 5.X Service Pack x

The version that is installed is listed in the **Version** column. The following list shows the current latest build number for each component:

- The App-V Client (as of 03/06/2018): 5.1.134.0 (App-V 5.1 March 2018 service release).
- The App-V Sequencer (as of 10/10/2017): 5.1.129.0 (App-V 5.1 September 2017 servicing release).
- The App-V Server components (as of 07/01/2017): 5.1.129.0 (App-V 5.1 September 2017 servicing release).

History of App-V release versions and dates:

Title	Build version	KB article	Release date
AppV 5.1 March 2018 service release	5.1.134.0	4074878	3/6/2018
App-V 5.1 September 2017 servicing release	5.1.129.0	4041137	10/10/2017
App-V 5.1 June 2017 servicing release	5.1.126.0	4018510	6/28/2017
App-V 5.1 March 2017 servicing release	5.1.118.0	4014009	3/30/2017

Title	Build version	KB article	Release date
App-V 5.1 December 2016 servicing release	5.1.116.0	3198158	12/09/2016
App-V 5.1 September 2016 servicing release	5.1.115.0	3168628	09/22/16
App-V 5.1 HF05	5.1.108.0	3172672	07/13/16
App-V 5.1 HF02	5.1.101.0	3139245	01/29/2016
App-V 5.1 HF01	5.1.99.0	3115834	11/23/2015
App-V 5.1 RTM	5.1.86.0	About 5.1	8/17/2015
App-V 5.0 SP3 HF03	5.0.10345.0	3172672	6/23/16
App-V 5.0 SP3	5.0.10107.0	About SP3	10/30/2014
App-V 5.0 SP2 HF05	5.0.3404.0	2963211	05/22/2014
App-V 5.0 SP2 HF04	5.0.3400.0	2956985	04/24/2014
App-V 5.0 SP2	5.0.3361.0	About SP2	12/02/2013
App-V 5.0 RTM	5.0.285.0	About App-V 5.0	11/1/2012

HTTP Error 500.19 - Internal Server Error when launching the App-V Management console

Article • 09/29/2021 • 2 minutes to read

This article provides a solution to an issue where launching the App-V 5.0 Management console that's installed on a drive other than the C: drive fails.

Applies to: Windows Server 2008 R2 Service Pack 1, Windows 7 Service Pack 1
Original KB number: 2800730

Symptoms

When the App-V 5.0 Management console is installed on a drive other than the C: drive, launching the console may fail and generate the following error message:

> HTTP Error 500.19 - Internal Server Error
> Module IIS Web Core
> Notification Unknown
> Handler Not yet determined
> Error Code 0x80070005
> Config Error Cannot read configuration file due to insufficient permissions
> Config File \\?\E:\Program Files\Microsoft Application Virtualization Server\ManagementService\web.config

Cause

This occurs due to invalid NTFS permissions on the drive hosting the App-V 5.0 Management Service INSTALLDIR directory.

Resolution

To resolve this issue, give the local computers Users group Read & execute, List folder contents and Read permissions to the root of the drive the hosts the App-V Management consoles INSTALLDIR directory. The INSTALLDIR parameter can be found referencing the following registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AppV\Server\ManagementService`

The local computer User group contains the following users by default:

- Local Administrator Account
- NT AUTHORITY\Authenticated users (S-1-5-11)
- NT AUTHORITY\INTERACTIVE (S-1-5-4)
- Domain\Domain users

After updating the permissions on the drive that hosts the INSTALLDIR directory, either stop and start the Microsoft App-V Management Service website in IIS or issue an IISRESET.

More information

Process Monitor can be used to troubleshoot these types of issues.

For more information, see Process Monitor v3.60.

How to troubleshoot applications failing to stream from an App-V management server

Article • 09/29/2021 • 6 minutes to read

This article describes how to troubleshoot virtualized applications in Microsoft Application Virtualization (App-V) that fail to stream from the management server.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2615139

Symptoms

When an application fails to stream on an App-V client, the application will fail to launch with the following error:

> The Application Virtualization Client could not launch *application name*.

The error message will also include an error description and code like the examples below:

> No connection could be made because the target machine actively refused it.
> Error code: xxxxxxx-xxxxxx2A-0000274D
>
> The package requested could not be found in the system data store or the files associated with this package could not be found on the server. Report the following error code to your System Administrator.
> Error code: xxxxxxx-xxxxxx0A-20000194
>
> No such host is known.
> Error Code: xxxxxxx-xxxxxx2A-00002AF9
>
> The specified Application Virtualization Server could not be accessed.
> Try again in a few minutes. If the problem persists, report the following error code to your System Administrator.
> Error Code: xxxxxxx-xxxxxx0A-10000002

In the Sftlog.txt file, the following error will be logged:

> [08/24/2011 15:32:56:618 JGSW ERR] {hap=5:app=Appname:tid=16C:usr=Administrator} The Application Virtualization Client could not connect to stream URL 'rtsp://appv-svr:554/Application/Application.sft' (rc 19D07F2A-0000274D, original rc 19D07F2A-0000274D).

> **Note**
>
> The error code in the Sftlog.txt will vary.

The first step in troubleshooting an application failing to stream is to determine if the issue is isolated to a single application or all applications.

Once the scope of the applications affected is determined, perform the steps below that are appropriate for your scenario.

Troubleshoot a single application that fails to stream

1. Review the Sftlog.txt file on the App-V client.

   On the App-V client, review the Sftlog.txt file on the App-V client. This log file may include additional information that wasn't included in the error message.

   The default location for the Sftlog.txt is: %systemdrive%\ProgramData\Microsoft\Application Virtualization Client.

2. Review the application .osd file on the App-V Management Server.

   a. On the App-V Management Server, open the application .osd file and scroll down to the following line:

      <CODEBASE HREF="rtsp://servername:554/ApplicationDirectory/Application.sft">

   b. Verify the protocol, sever name, port and path to the SFT file are correct.

      Default ports for each protocol type:

      - RTSP=554
      - RTSPS=322
      - HTTP=80

- HTTPS=443

c. If changes were made to the application .osd file, save the changes and then open the Application Virtualization Client MMC snap-in on the App-V client and refresh the Publishing Server.

d. Launch the application on the App-V client to see if the error continues to occur.

> ⓘ **Note**
>
> If the application OSD file is using the %SFT_SOFTGRIDSERVER% environment variable for the server name, verify the environment variable is configured on the App-V client.

3. Delete the application from the cache on the App-V client.
   a. On the App-V client, open the Application Virtualization Client snap-in that's located under Administrative Tools.
   b. Click **Applications**.
   c. Right-click the application that is failing to stream and click **Delete**.
   d. Click **Yes** when you receive the confirmation dialog box.
   e. Once the application is deleted, refresh the publishing server to republish the application.

   To refresh the publishing server, perform one of the following methods:

   - Method 1
     a. Open the Application Virtualization Client snap-in.
     b. Click **Publishing Servers**.
     c. Right-click the publishing server and choose **Refresh Server**.
   - Method 2
     a. Right-click the App-V icon in the notification area and choose **Refresh Applications**.
     b. Launch the application on the App-V client to see if the error continues to occur.

Troubleshoot all applications failing to stream

1. Review the Sftlog.txt file on the App-V client.

   On the App-V client, review the Sftlog.txt file on the App-V client. This log file may include additional information that wasn't included in the error message.

The default location for the Sftlog.txt is %systemdrive%\ProgramData\Microsoft\Application Virtualization Client.

2. Verify the App-V client can access the content directory.

   On the App-V client, click **Start**, in the **Search** or **Run** line, type the UNC path of the content share (For example: \\appv-svr\content) and then press ENTER.

   If the client fails to connect to the content share, verify the UNC path is correct and verify the NTFS and Share permissions on the content directory are correct by performing the steps below.

   On the server hosting the content directory, verify the following NTFS and Share permissions are configured on the content directory:

   - App-V Users = Read
   - App-V Administrators = Read and Write
   - Network Service = Read and Write

   The default location for the content directory is: %systemdrive%\Program Files (x86)\Microsoft System Center App Virt Management Server\App Virt Management Server\content.

3. Verify the path to the content directory on the App-V Management Server. To verify this, perform the following steps on the App-V Management Server:
   a. In Administrative Tools, open the Application Virtualization Management Console.
   b. Right-click the server name and then click **System Options**.
   c. Verify the **Default Content Path** is pointing to the content directory location.

      > ⓘ **Note**
      >
      > The content location should be referenced by UNC path (For example: \\appv-svr\content).

   d. Click **OK** to close the **System Options** window.
   e. Close the Application Virtualization Management Console.
   f. Open Regedit.
   g. Navigate to the following key:

      - 32-bit systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SoftGrid\4.5\Server`
      - 64-bit systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\SoftGrid\4.5\Server`

h. Verify the SOFTGRID_CONTENT_DIR registry value is pointing to the content directory location.

> ⓘ **Note**
>
> The content location should be referenced by UNC path if the content share is a DFS share (For example: \\appv-svr\content).

i. If the SOFTGRID_CONTENT_DIR registry value was modified, restart the Application Virtualization Management Server service or restart the server.

4. Verify the Application Virtualization Management Server service is started on the App-V Management Server. To verify this, perform the following steps on the App-V Management Server:
   a. In Administrative Tools, open the Services MMC snap-in.
   b. Locate the Application Virtualization Management Server service.
   c. Verify that the service is Started.
   d. If the service is not started, right-click Application Virtualization Management Server, and then click **Start**.
   e. If the service fails to start, search the Microsoft Knowledge Base for the error message that is reported.

5. Verify the App-V client can telnet to the App-V Management Server and port. To verify this, perform the following steps on the App-V client:

   a. At a command prompt, type `telnet ServerName Port`, and then press ENTER.

      For example, type the `telnet appv-svr 554` command and then press ENTER.

   b. If the connection succeeds, the window is blank. Press ENTER two times and you will receive the following message:

      ```
      RTSP/1.0 400 Bad Request
      Server: Microsoft Application Virtualization Server/x.x.x.xxxxx [Win32;
      Windows NT x.x]
      Date: xxx, xx xxx xxxx xx:xx:xx xxx
      ```

      If the connection is unsuccessful, you will receive the following message:

      ```
      Could not open connection to the host, on port 554: Connect failed
      ```

      If the Application Virtualization Management Server service is started but the client cannot telnet to the server, verify that port traffic between the client and

the server is not restricted by a firewall or by other software. For more information, contact the network administrator.

6. Review the application .osd files on the App-V Management Server.

   a. On the App-V Management Server, open the application .osd file and scroll down to the following line:

      <CODEBASE HREF="rtsp://servername:554/ApplicationDirectory/Application.sft">

   b. Verify that the protocol, sever name, port and path to the SFT file are correct.

      Default ports for each protocol type:

      - RTSP= 554
      - RTSPS=322
      - HTTP=80
      - HTTPS=443

   c. If changes were made to the application .osd file, save the changes and then open the Application Virtualization Client MMC snap-in on the App-V client and refresh the Publishing Server.

   d. Repeat steps 1-3 for all applications that fail to stream.

> ⓘ **Note**
>
> If the application OSD file is using the %SFT_SOFTGRIDSERVER% environment variable for the server name, verify the environment variable is configured on the App-V Client.

7. Clear the cache on the App-V client.

   If steps 2-6 have confirmed that the App-V client can communicate with the App-V Management Server and the settings are configured properly, it's possible that the application is failing to stream due to a corrupted cache file on the App-V client.

> ⓘ **Note**
>
> Clearing the cache on the App-V client will delete all application data from the cache file. This may cause application load times to increase the first time an application is launched after the cache is cleared.

To clear the cache on the App-V client, perform the following steps:

a. Open Regedit.

b. Navigate to the following key:

- 32-bit systems: `HKEY_LOCAL_MACHINE\Software\Microsoft\Softgrid\4.5\Client\AppFS`
- 64-bit systems: `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\SoftGrid\4.5\Client\AppFS`

c. Double-click the value name State and change the value data to 0.

d. Restart the App-V client computer.

Additional resources

For more information about Hyper-V, see Hyper-V.

Common error codes when an application fails to stream:

- 44-00001004
- 0a-00000193
- 0a-10000001
- 0a-0000e02b
- 0a-200001f4
- 64-00000003
- 2A-80090322
- 08-10000003
- 0a-0000E005
- 0A-0000E0A3
- 0A-40000191
- 2A-0000274D
- 0A-20000194
- 2A-00002AF9
- 0A-10000002

Adding a package version in Microsoft Application Virtualization returns error 0x8007012F

Article • 09/29/2021 • 2 minutes to read

This article provides help to work around an issue where you receive error 0x8007012F when you remove and then add the same package version in the Microsoft Application Virtualization console.

Applies to: Windows Server 2008 R2 Service Pack 1, Windows 7 Service Pack 1
Original KB number: 2780304

Symptoms

Removing and then adding the same package version in the Microsoft Application Virtualization console fails and returns error 0x8007012F.

Cause

When an App-V v5 package version is added, the package files are created in %programdata%\App-V\{PackagID}\{VersionId}. When the package version is removed, the package files in %programdata%\App-V are also removed. Any files that the App-V v5 client is unable to remove are marked for deletion at the next system restart.

If all of the package version files were successfully removed, then the same package version can be added immediately without a system restart, however if any of the files could not be removed then adding the same package version that was just deleted returns error 0x8007012F. This is by design.

Workaround

To work around this issue, reboot the computer before adding the same package version again. The system restart will complete the removal of the package version after which the same package version can be successfully added again.

This scenario is most likely to occur in a test environment as in production there's no reason to remove a package version and then add the same package version again. However, if this were to occur in production and if a system restart cannot be

performed, there is an alternative workaround that does not require a system restart. As an alternative, you can create a new version of the same package. To do this, open the package in the Sequencer and then save it. The new package version will not be affected by the partially deleted state of the prior version and so it can be added without restarting the system.

> **Note**
>
> If this problem occurs in a full infrastructure scenario then at the next "Refresh" this error will be logged in the App-V Client Admin event log.

How to remove a cached copy of an unpublished package in Microsoft App-V v5

Article • 09/29/2021 • 2 minutes to read

This article describes how to remove a cached copy of an unpublished package in Microsoft App-V v5.

Applies to: Windows 10 - all editions
Original KB number: 2768945

Summary

When a previously published package is unpublished from the Microsoft Application Virtualization (App-V) Management Server, all entry points (for example, Shortcuts, FTA's, etc.) for that package are removed from the App-V client, however the cached copy of the package is not removed (deleted) from %programdata%\App-V\{PkGID}\{VerID}.

Also when a new version of a previously cached package is streamed, the older version of the cache is not removed. Instead, hard links are between the package files that have remained unchanged between the different versions.

> **Note**
>
> The folder %programdata%\App-V is the default path for PackageInstallationRoot. To check the path run `Get-AppvClientConfiguration` and examine the value of PackageInstallationRoot.

At times, you might want to remove unpublished packages from the computer (for example, to reclaim lost disk space). You can remove packages by running the PowerShell command `Remove-AppvClientPackage`. Much like uninstall native applications, the `Remove-AppvClientPackage` must be run with administrative rights.

More Information

`Remove-AppvClientPackage` supports the following inputs for the package:

- Name
- PackageID
- Version
- VersionID

To find the values the parameters listed above, you can make use of `Get-AppvClientPackage -All` . The output is a list of all packages that are present on the computer.

> **Note**
>
> 1. The -All switch is needed to list the unpublished packages.
> 2. Also the publishing status is checked for the user in whose context the command is being run.
> 3. Virtual Applications which are installed via MSI should be removed from Add Remove Programs. You should not remove them by using Remove-AppvClientPackage.

From a PowerShell prompt run: `Get-AppvClientPackage -all`. It should return something similar to the following:

PowerShell

```
PS C:\temp> Get-AppvClientPackage -All

PackageId : x1x1x1x1-x1x1-x1x1-x1x1-x1x1x1x1x1x1
VersionId : x2x2x2x2-x2x2-x2x2-x2x2-x2x2x2x2x2x2
Name : MyVirtualPackage
Version : 0.0.0.1
Path : c:\temp\MyVirtualPackage.appv
IsPublishedToUser : False
UserPending : False
IsPublishedGlobally : False
GlobalPending : False
InUse : False
InUseByCurrentUser : False
PackageSize : 1234567
PercentLoaded : 100
IsLoading : False
HasAssetIntelligence : True

PackageId : y1y1y1y1-y1y1-y1y1-y1y1-y1y1y1y1y1y1
VersionId : y2y2y2y2-y2y2-y2y2-y2y2-y2y2y2y2y2y2
Name : MyVirtualPackage
Version : 0.0.0.2
Path : c:\temp\MyVirtualPackage_2.appv
```

```
IsPublishedToUser : False
UserPending : False
IsPublishedGlobally : False
GlobalPending : False
InUse : False
InUseByCurrentUser : False
PackageSize : 1234900
PercentLoaded : 100
IsLoading : False
HasAssetIntelligence : True
```

To remove the older version of the MyVirtualPackage package, run the following:

To remove a package using the PackageID, run this:

PowerShell

```
Remove-AppVClientPackage - x1x1x1x1-x1x1-x1x1-x1x1-x1x1x1x1x1x1
```

Just be sure to modify the Version and Package IDs used above so that they reflect the correct package you are trying to remove.

To remove all packages, including all Versions of all packages irrespective of their publishing status run the following:

PowerShell

```
Get-AppvClientPackage -All | Remove-AppVClientPackage
```

How to troubleshoot publishing server refresh failures in App-V v5

Article • 09/29/2021 • 5 minutes to read

This article describes how to troubleshoot publishing server refresh failures in Microsoft Application Virtualization (App-V) v5.

Applies to: Windows 10 - all editions
Original KB number: 2778168

Summary

Perform the steps listed below to troubleshoot this issue.

Step 1: Verify the publishing server URL configured on the client

To verify the publishing server URL, perform the following steps:

1. On the App-V Client, open an elevated PowerShell command prompt.
2. Type *Get-AppvPublishingServer* and hit enter.
3. Verify the URL listed in the output is correct.

   If the publishing server name is PubSvr and the publishing server port is 82, the URL listed in the `Get-AppvPublishingServer` output should be: `http://PubSvr:82` or `https://PubSvr:82`

If the publishing server URL is incorrect, use the `Remove-AppvPublishingServer` cmdlet to remove the publishing server. Then use the `Add-AppvPublishingServer` cmdlet to add the publishing server with the correct URL.

Sample commands to remove and readd the publishing server:

PowerShell

```
Remove-AppvPublishingServer -ServerId 1
Add-AppvPublishingServer -Name PublishingSever -URL http://PubSvr:82
```

Common errors that are logged on the App-V client if the publishing server URL is incorrect:

- PowerShell

> Sync-AppvPublishingServer: Application Virtualization Service failed to complete requested operation.
> Operation attempted: RefreshPublishingServer.
> Internet Error: 0x80072EE7 - The server name or address could not be resolved.
> Error module: Publishing. Internal error detail: 45500D2780072EE7.
> Please consult AppV Client Event Log for more details.

> Sync-AppvPublishingServer: Application Virtualization Service failed to complete requested operation.
> Operation attempted: RefreshPublishingServer.
> AppV Error Code: 0500090001.
> Error module: Shared Component. Internal error detail: 3E50110500090001.
> Please consult AppV Client Event Log for more details.

- APP-V Event Log

> Log Name: Microsoft-AppV-Client/Admin
> Source: Microsoft-AppV-Client
> Event ID: 19102
> Task Category: Publishing Refresh
> Level: Error
> Description:
> Getting server publishing data failed.
> URL: `http://PubSvr:82/`
> Error code: 0x45500D27 - 0x80072EE7

> Log Name: Microsoft-AppV-Client/Admin
> Source: Microsoft-AppV-Client
> Event ID: 19203
> Task Category: Publishing Refresh
> Level: Error
> Description:
> HttpRequest sendRequest failed.
> URL: `http://PubSvr:82/`
> Error code: 0x45500D27 - 0x80072EE7

> Log Name: Microsoft-AppV-Client/Admin
> Source: Microsoft-AppV-Client
> Event ID: 19205
> Task Category: Publishing Refresh
> Level: Error
> Description:
> The content from server is not valid XML for publishing.
> URL: `http://PubSvr:82/`
> Error code: 0x3E501105 - 0x90001

> Log Name: Microsoft-AppV-Client/Admin
> Source: Microsoft-AppV-Client
> Event ID: 19102
> Task Category: Publishing Refresh
> Level: Error
> Description:
> Getting server publishing data failed.
> URL: `http://PubSvr:82/`
> Error code: 0x3E501105 - 0x90001

Step 2: Add Windows Firewall exception on the publishing server

If the Windows Firewall is enabled on the publishing server, an Inbound Rule must be added to allow inbound connections on the port used by the publishing server.

To add an **Inbound Rule**, perform the following steps:

1. On the publishing server, open the **Windows Firewall**.
2. Click **Advanced Settings**.
3. Right-click on **Inbound Rules** and select **New Rule**.
4. Select **Port** and click **Next**.
5. Select **TCP**, specify the port used by the publishing server and click **Next**.
6. Select the appropriate connection condition for your environment and click **Next**.
7. Select the appropriate profile and click **Next**.
8. Provide a name for the **Inbound Rule** and click **Finish**.

Common errors that are logged on the App-V client if the firewall port is blocked:

- PowerShell

> Sync-AppvPublishingServer : Application Virtualization Service failed to complete requested operation.
> Operation attempted: RefreshPublishingServer.
> Internet Error: 0x80072EE2 - The operation timed out
> Error module: Publishing. Internal error detail: 45500D2780072EE2.
> Please consult AppV Client Event Log for more details.

- App-V Event Logs

> Log Name: Microsoft-AppV-Client/Admin
> Source: Microsoft-AppV-Client
> Event ID: 19102
> Task Category: Publishing Refresh
> Description:
> Getting server publishing data failed.
> URL: `http://PubSvr:82/`
> Error code: 0x45500D27 - 0x80072EE2

> Log Name: Microsoft-AppV-Client/Admin
> Source: Microsoft-AppV-Client
> Event ID: 19203
> Task Category: Publishing Refresh
> Description:
> HttpRequest sendRequest failed.
> URL: `http://PubSvr:82/`
> Error code: 0x45500D27 - 0x80072EE2

Step 3: Verify the publishing server site is started on the publishing server

To verify the publishing server site is started, perform the following steps:

1. On the publishing server, open the **IIS Manager** console.
2. Click **Sites**.
3. Verify the **Microsoft App-V Publishing Service** site is **Started**.

Common errors that are logged on the App-V client if the publishing server site is not started:

- PowerShell

> Sync-AppvPublishingServer : Application Virtualization Service failed to complete requested operation.
> Operation attempted: RefreshPublishingServer.
> Internet Error: 0x80072EE2 - The operation timed out
> Error module: Publishing. Internal error detail: 45500D2780072EE2.
> Please consult AppV Client Event Log for more details.

- App-V Event Logs

> Log Name: Microsoft-AppV-Client/Admin
> Source: Microsoft-AppV-Client
> Event ID: 19102
> Task Category: Publishing Refresh
> Level: Error
> Description:
> Getting server publishing data failed.
> URL: `http://PubSvr:82/`
> Error code: 0x45500D27 - 0x80072EE2

> Log Name: Microsoft-AppV-Client/Admin Source: Microsoft-AppV-Client Event ID: 19203 Task Category: Publishing Refresh Level: Error Description: HttpRequest sendRequest failed. URL: `http://PubSvr:82/` Error code: 0x45500D27 - 0x80072EE2

Step 4: Verify the publishing server application pool is started on the publishing server

To verify the publishing server application pool is started, perform the following steps:

1. On the publishing server, open the **IIS Manager** console.
2. Click **Application Pools**.
3. Verify the **AppVPublishing application pool** is **Started**.

Common errors that are logged on the App-V client if the **AppVPublishing application pool** is not started:

- PowerShell

> Sync-AppvPublishingServer : Application Virtualization Service failed to complete requested operation.
> Operation attempted: RefreshPublishingServer.

> Windows Error: 0x801901F7 -
> Error module: Publishing. Internal error detail: 45500D27801901F7.
> Please consult AppV Client Event Log for more details.

- App-VEvent Logs

> Log Name: Microsoft-AppV-Client/Admin
> Source: Microsoft-AppV-Client
> Event ID: 19102
> Task Category: Publishing Refresh
> Level: Error
> Description:
> Getting server publishing data failed.
> URL: `http://PubSvr:82/`
> Error code: 0x45500D27 - 0x801901F7

> Log Name: Microsoft-AppV-Client/Admin
> Source: Microsoft-AppV-Client
> Event ID: 19203
> Task Category: Publishing Refresh
> Level: Error
> Description:
> HttpRequest sendRequest failed.
> URL: `http://PubSvr:82/`
> Error code: 0x45500D27 - 0x801901F7

Step 5: Verify the publishing server URL is accessible using a web browser

On the App-V client, access the publishing server URL (for example, `http://PubSvr:82/`) using a web browser. If the publishing server is working properly and is accessible, an XML output will be displayed which lists the applications published on the publishing server:

XML

```
- <Publishing Protocol="1.0">
- <Packages>
  <Package PackageId="639138dd-a4f5-4846-bab2-02e94a87c8a6"
VersionId="b29da9c2-07d1-4fac-97ca-4f081c487c79"
PackageUrl="\\pubsvr\content\Office 2013 AppV
Package\ProPlusVolume_VisioProVolume_ProjectProVolume_en-us_x86.appv" />
```

```
  </Packages>
- <NoGroup>
  <Package PackageId="639138dd-a4f5-4846-bab2-02e94a87c8a6" />
  </NoGroup>
  </Publishing>
```

In the example above, Office 2013 is the only package currently published on the publishing server.

Step 6: Perform a publishing server refresh

After performing the steps above, perform a manual publishing refresh to verify no errors are logged.

There are two methods to manually perform a publishing refresh:

- In PowerShell, use the `Sync-AppvPublishingServer` cmdlet.
- In the App-V client console, click **Update**.

> ⓘ **Note**
>
> The Update box will be greyed out if a publishing server hasn't been configured on the client machine.

Backup and Storage troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Backup and Storage-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Backup and Storage sub categories

- Configuring and using Backup software
- Partition and volume management
- Storage hardware
- System Restore or resetting your computer
- Volume Shadow Copy Service (VSS)

Backup fails when you try to create a system image

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where backup fails when you try to create a system image.

Applies to: Windows 7 Service Pack 1
Original KB number: 2696906

Symptoms

Consider the following scenario:

- You are running Windows 7 Service Pack 1.
- In the Backup and Restore Control Panel applet, you click on the link to "Create a system image".
- The source volume that you are imaging is 2 terabytes in size or larger.

In this scenario, after the backup process has started, you may see an error similar to the following:

> The backup failed.
>
> Volumes larger than 2088958 megabyes cannot be protected. (0x807800B4)

The only option is to close the dialog box and exit out of the **Create a system image** wizard.

Cause

When creating a system image in Windows 7 Service Pack 1 by using the **Create a system image** wizard, a virtual hard disk (.vhd) is created and the system image is written to it. The current virtual hard disk specification limits the size of a virtual hard disk to be 2040 GB, which can fit a volume size of 2040 GB - 2 MB (that is, 2088958 MB). Due to this limitation, the source volume size must be 2,088,958 MB or less for the system image to be created.

Note

All of the above values are slightly under 2 TB in size (2 TB = 2048 GB = 2097152 MB).

Resolution

To work around this limit, shrink your volume size to 2,088,958 MB or less prior to creating the system image. More information on shrinking a basic volume can be found in the following article:

Shrink a Basic Volume

Error code 0x81000031 occurs when you try to back up files by using the Backup and Restore Wizard on a Windows 7-based computer

Article • 09/23/2021 • 3 minutes to read

This article describes a problem that occurs when you use the Backup and Restore Wizard in Windows 7 to back up files to an external hard disk drive.

Applies to: Windows 7 Service Pack 1
Original KB number: 975692

Symptoms

Consider the following scenarios.

Scenario 1: Custom libraries are unavailable

- You have a computer that is running Windows 7.
- You add a custom library that is located on a removable drive or on a network drive.
- You try to perform a backup when one or more of your custom libraries isn't available.

In this scenario, when you try to back up your files by using the Windows Backup and Restore Wizard, you receive an error message that resembles the following message:

> Error code: 0x81000031

Scenario 2: BitLocker Drive Encryption is enabled

- You have a computer that is running Windows 7.
- You connect an external hard disk drive to the computer.
- You enable Windows BitLocker Drive Encryption on the system drive.

In this scenario, when you try to back up your files to the external drive by using the Windows Backup and Restore Wizard, you receive an error message that resembles the following message:

> BitLocker Drive Encryption cannot be used because critical BitLocker system files are missing or corrupted.
>
> Error code: 0x81000031

Cause

Scenario 1: Custom libraries are unavailable

This problem can occur if you have added custom libraries that aren't accessible when you perform a backup by using Windows Backup Wizard. Custom libraries can become unavailable if those libraries are located on a network drive that is unavailable, or if those libraries are located on removable media.

Scenario 2: BitLocker Drive Encryption is enabled

This problem occurs because the BitLocker Wizard moves Windows Recovery Environment (Windows RE) from the system drive to the external hard disk drive. This prevents creating a backup on the external hard disk.

Workaround

To work around this problem, follow the appropriate steps for your scenario.

Scenario 1: Custom libraries are unavailable

To reset your libraries to the default libraries (Documents, Music, Pictures, and Videos), follow these steps:

1. Click Start, and then click **Computer**.
2. Right-click **Libraries** from the navigation pane on the left side of the Explorer window, and then click **Restore Default Libraries**.

   > ⓘ **Note**
   >
   > This operation removes any custom libraries that are in your libraries location. You can restore these libraries when the library locations become available again.

3. Start the Backup and Restore Wizard to back up your files and data.

Scenario 2: BitLocker Drive Encryption is enabled

To disable and re-enable BitLocker Drive Encryption, follow these steps:

1. Connect the external hard disk drive to the computer. Make sure that the external hard disk drive is powered on.

2. Create a Windows 7 system repair disc. To do this, follow these steps:
   a. Click **Start**, and then type create a system repair disc in the **Start Search** box.
   b. In the **Programs** list, click **Create a System Repair Disc**.
   c. Follow the instructions on the screen to create the disc.

   > ⓘ **Note**
   >
   > You must have a CD or DVD burner to create a system repair disc.

3. Start an elevated command prompt. To do this, follow these steps:
   a. Click **Start**, and then type command prompt in the **Start Search** box.
   b. In the **Programs** list, right-click **Command Prompt**, and then click **Run as administrator**.

4. At the elevated command prompt, type the following command, and then press ENTER:

   Console

   ```
   C:\Windows\System32\REAgentC.exe /disable
   ```

5. Disconnect the external hard disk drive.

6. At the elevated command prompt, type the following command, and then press ENTER:

   Console

   ```
   C:\Windows\System32\REAgentC.exe /enable
   ```

   > ⓘ **Note**

> This operation might fail. In this case, use the Windows 7 system repair disc that you created in step 2 if you have to have access to recovery tools.

7. Reconnect the external hard disk drive to the computer.
8. Start the Backup and Restore Wizard to back up your files and data to the external hard disk drive.

More information

For more information about how to create and use a system repair disc, visit the following Microsoft Web site:

Create a system repair disc

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the "Applies to" section.

System Image Recovery fails with a 0x80070002 error

Article • 09/23/2021 • 2 minutes to read

This article describes a system image restore problem that occurs in Windows 8.1 when you try to recover from a backup that's stored on a partition on the system disk. A resolution is provided.

Applies to: Windows 8.1
Original KB number: 2989057

Symptoms

Consider the following scenario:

- You're running Windows 8.1, and you have the Windows 8.1 update (KB2919355) installed.
- You've taken a system image backup and saved it to a partition on the same disk as drive C.
- The partition that you saved the backup to is much smaller than drive C.

When you try to recover from the backup by using System Image Recovery, it fails and returns the following error:

> The system image restore failed.
> Error details: The system cannot find the file specified. (0x80070002)

Additionally, you can't start Windows after this error occurs.

Cause

The error occurs because the backup image is prematurely dismounted during the restore process.

Workaround

When you start the system after this error occurs, it generally goes into Automatic Repair mode. However, this process fails. To recover, follow these steps:

1. Click **Advanced options**.
2. Under **Choose an option**, click **Troubleshoot**, click **Advanced options**, and then click **Command Prompt**.
3. Using DISKPART, locate the volume where the OS was installed. After the problem occurs, the volume will be recognized as a RAW volume (drive C in the following example).

```
Console

X:\Windows\System32>diskpart

Microsoft DiskPart version 6.3.9600

Copyright (C) 1999-2013 Microsoft Corporation.
On computer: MININT-NS2UFF8

DISKPART> list volume

 Volume ###  Ltr Label       Fs    Type        Size   Status    Info
 ----------  --- ----------- ----- ----------  ------- --------- --------
 Volume 0 E DVD-ROM 0 B No Media
 Volume 1 C RAW Partition 2970 GB Healthy
 Volume 2 D New Volume NTFS Partition 29 GB Healthy
 Volume 3 Recovery NTFS Partition 300 MB Healthy Hidden
```

> **Note**
>
> The drive letters may differ in your installation of Windows.

4. Format the RAW volume:

```
Console

DISKPART> select volume 1

Volume 1 is the selected volume.

DISKPART> format fs=NTFS quick

100 percent completed
```

5. Exit DISKPART, and then close the command prompt:

```
Console
```

```
DISKPART> exit

Leaving DiskPart...
```

6. Under **Choose an option**, click **Troubleshoot**, click **Advanced options**, and then click **System Image Recovery**.
7. Follow the steps in the Re-image Your Computer Wizard to complete the restore from the backup that you saved.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the "Applies to" section.

Microsoft regularly releases software updates to address specific bugs. If Microsoft releases a software update to resolve this bug, this article will be updated with additional information.

Access is denied error message appears when permissions are correct

Article • 09/23/2021 • 2 minutes to read

This article provides a solution for "access is denied" error message when permissions are correct.

Applies to: Windows Server 2003
Original KB number: 250494

Symptoms

When you try to access a file on an NTFS file system volume, you may receive an "access is denied" error message. The file's NTFS permissions indicate that you can access the file.

Cause

This behavior can occur if another user has encrypted the file. To determine if a file has been encrypted, see the "More Information" section in this article.

Resolution

To resolve this behavior, the file must be decrypted by the user who encrypted the file, or by the designated Recovery agent. Files that are encrypted by using the Encrypting File System (EFS) are accessible only to the person who encrypted the file, regardless of the other permissions that are on the file.

Status

This behavior is by design.

More Information

To determine if a file has been encrypted:

1. Start **Windows Explorer**, and then click **Detail** on the **View** menu to view the details of the folder's contents.

2. Click **Choose Columns** from the **View** menu, and then click to select the **Attributes** check box to add the **Attributes** column to the current view, and to view the file attributes.

If there is an "E" in the **Attributes** column for that file, the file is encrypted.

Event ID 8 is logged in the Application log

Article • 09/23/2021 • 3 minutes to read

This article provides help to solve the Event ID 8 logged in the Application log.

Applies to: Windows 10 - all editions
Original KB number: 317541

Symptoms

One or both of the following event messages may be logged in the Application log:

- Message 1

> Event Type: Error
> Event Source: crypt32
> Event Category: None
> Event ID: 8
> Date: *date*
> Time: *time*
> User: *user name*
> Computer: *computer name*
> Description:
> Failed auto update retrieval of third-party root list sequence number from: <`http://www.download.windowsupdate.com/msdownload/update/v3/static/trusteddr/en/authrootseq.txt`> with error: This operation returned because the timeout period expired. For more information, see Help and Support Center at `http://support.microsoft.com`.

- Message 2

> Event Type: Error
> Event Source: crypt32
> Event Category: None
> Event ID: 8
> Date: *date*
> Time: *time*
> User: *user name*

> Computer: *computer name*
> Description:
> Failed auto update retrieval of third-party root list sequence number from: <`http://www.download.windowsupdate.com/msdownload/update/v3/static/trusteddr/en/authrootseq.txt`> with error: The specified server cannot perform the requested operation. For more information, see Help and Support Center at `http://support.microsoft.com`.

Cause

This behavior can occur if the Update Root Certificates component is turned on and the computer cannot connect to the Windows Update server on the Internet. The Update Root Certificates component automatically updates trusted root-certificate authorities from the Microsoft Update server at regular intervals.

Resolution

To resolve this behavior, you must connect to the Internet or turn off the Update Root Certificates component. To turn off the Update Root Certificates component, follow these steps:

1. In Control Panel, double-click **Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. Clear the **Update Root Certificates** check box, and then continue with the Windows Components Wizard.

Status

This behavior is by design.

More information

The Update Root Certificates component uses the WinHTTP API to communicate with the Windows Update server. If your computer is behind a proxy server, you may have to set the proxy settings by using the Proxycfg.exe utility. To configure WinHTTP by using Proxycfg.exe, follow these steps:

1. Start the Proxycfg.exe utility from the <Systemroot>\System32 folder. If you cannot locate the Proxycfg.exe utility in the <Systemroot>\System32 folder, see ProxyCfg.exe Proxy Configuration Tools.

2. Determine the proxy server name that you use.

3. At the command prompt, configure your computer by using the Proxycfg.exe utility with one of the following settings:

    - To see the current proxy settings for WinHTTP, type *proxycfg*, and then press RETURN. By default, the current proxy setting should be **Proxy Direct**. If you have Microsoft XML Parser (MSXML) 3.0 SP1 or earlier versions, the current proxy setting may be **Not Set**. In this scenario, type `proxycfg -d`, and then press RETURN to restore the default proxy settings for WinHTTP.

    - To not use any proxy servers when connecting server-to-server, type `proxycfg -d`, and then press RETURN.

    - To use a proxy server when connecting server-to-server, type `proxycfg -p`, type the proxy servers you want to use, and then press RETURN. Additionally, you can add optional bypass lists for servers that will not be accessed through a proxy. You can find acceptable proxy server formats or bypass formats in the the Proxycfg.exe utility ReadMe.txt file.

    - To import proxy information from the settings that Internet Explorer uses to connect to the Internet, also known as the WinInet settings, and to include this proxy information in the WinHTTP settings, type `proxycfg -u`, and then press RETURN.

4. Stop and restart Microsoft Internet Information Server (IIS).

The following are some command line examples using Proxycfg.exe:

- Example 1:

    Console

    ```
    proxycfg -d -p my Proxy Server :80 "<local>"
    ```

    This example shows the most common use for Proxycfg.exe. This command specifies that both HTTP and HTTPS servers must be accessed through the proxy server that is named *my Proxy Server* with a port number of 80, unless the host name does not contain a period. In this case, the `-d` option has no effect.

- Example 2:

    Console

    ```
    proxycfg -p my Proxy Server
    ```

This example specifies that both HTTP and HTTPS servers must be accessed through the proxy server that is named my Proxy Server. It specifies no bypass list.

- Example 3:

```
Console

proxycfg -p "http= http_proxy https= https_proxy" "
<local>;*.microsoft.com"
```

This example specifies that HTTP servers must be accessed through the *http_proxy*proxy, and that HTTPS servers must be accessed through *https_proxy*. Local intranet sites and host names that do not contain a period, and any site in the .microsoft.com domain, bypass the proxy.

For more information about how to troubleshoot problems with Internet connections, see Fix Wi-Fi connection issues in Windows.

Overview of FAT, HPFS, and NTFS File Systems

Article • 09/23/2021 • 12 minutes to read

This article explains the differences between File Allocation Table (FAT), High Performance File System (HPFS), and NT File System (NTFS) under Windows NT, and their advantages and disadvantages.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 100108

> **Note**
>
> HPFS is only supported under Windows NT versions 3.1, 3.5, and 3.51. Windows NT 4.0 does not support and cannot access HPFS partitions. Also, support for the FAT32 file system became available in Windows 98/Windows 95 OSR2 and Windows 2000.

FAT overview

FAT is by far the most simplistic of the file systems supported by Windows NT. The FAT file system is characterized by the file allocation table (FAT), which is really a table that resides at the very "top" of the volume. To protect the volume, two copies of the FAT are kept in case one becomes damaged. In addition, the FAT tables and the root directory must be stored in a fixed location so that the system's boot files can be correctly located.

A disk formatted with FAT is allocated in clusters, whose size is determined by the size of the volume. When a file is created, an entry is created in the directory and the first cluster number containing data is established. This entry in the FAT table either indicates that this is the last cluster of the file, or points to the next cluster.

Updating the FAT table is very important as well as time consuming. If the FAT table is not regularly updated, it can lead to data loss. It is time consuming because the disk read heads must be repositioned to the drive's logical track zero each time the FAT table is updated.

There is no organization to the FAT directory structure, and files are given the first open location on the drive. In addition, FAT supports only read-only, hidden, system, and

archive file attributes.

FAT naming convention

FAT uses the traditional 8.3 file naming convention and all filenames must be created with the ASCII character set. The name of a file or directory can be up to eight characters long, then a period (.) separator, and up to a three character extension. The name must start with either a letter or number and can contain any characters except for the following:

```
. " / \ [ ] : ; | = ,
```

If any of these characters are used, unexpected results may occur. The name cannot contain any spaces.

The following names are reserved:

CON, AUX, COM1, COM2, COM3, COM4, LPT1, LPT2, LPT3, PRN, NUL

All characters will be converted to uppercase.

Advantages of FAT

It is not possible to perform an undelete under Windows NT on any of the supported file systems. Undelete utilities try to directly access the hardware, which cannot be done under Windows NT. However, if the file was located on a FAT partition, and the system is restarted under MS-DOS, the file can be undeleted. The FAT file system is best for drives and/or partitions under approximately 200 MB, because FAT starts out with very little overhead. For further discussion of FAT advantages, see the following:

- Windows NT Server "Concepts and Planning Guide," Chapter 5, section titled "Choosing a File System"
- Windows NT Workstation 4.0 Resource Kit, Chapter 18, "Choosing a File System"
- Windows NT Server 4.0 Resource Kit "Resource Guide," Chapter 3, section titled "Which File System to Use on Which Volumes"

Disadvantages of FAT

Preferably, when using drives or partitions of over 200 MB the FAT file system should not be used. This is because as the size of the volume increases, performance with FAT will quickly decrease. It is not possible to set permissions on files that are FAT partitions.

FAT partitions are limited in size to a maximum of 4 Gigabytes (GB) under Windows NT and 2 GB in MS-DOS.

For further discussion of other disadvantages of FAT, see the following:

- Windows NT Server "Concepts and Planning Guide," Chapter 5, section titled "Choosing a File System"
- Windows NT Workstation 4.0 Resource Kit, Chapter 18, "Choosing a File System"
- Microsoft Windows NT Server 4.0 Resource Kit "Resource Guide," Chapter 3, section titled "Which File System to Use on Which Volumes"

HPFS overview

The HPFS file system was first introduced with OS/2 1.2 to allow for greater access to the larger hard drives that were then appearing on the market. Additionally, it was necessary for a new file system to extend the naming system, organization, and security for the growing demands of the network server market. HPFS maintains the directory organization of FAT, but adds automatic sorting of the directory based on filenames. Filenames are extended to up to 254 double byte characters. HPFS also allows a file to be composed of "data" and special attributes to allow for increased flexibility in terms of supporting other naming conventions and security. In addition, the unit of allocation is changed from clusters to physical sectors (512 bytes), which reduces lost disk space.

Under HPFS, directory entries hold more information than under FAT. As well as the attribute file, this includes information about the modification, creation, and access date and times. Instead of pointing to the first cluster of the file, the directory entries under HPFS point to the FNODE. The FNODE can contain the file's data, or pointers that may point to the file's data or to other structures that will eventually point to the file's data.

HPFS attempts to allocate as much of a file in contiguous sectors as possible. This is done in order to increase speed when doing sequential processing of a file.

HPFS organizes a drive into a series of 8-MB bands, and whenever possible a file is contained within one of these bands. Between each of these bands are 2K allocation bitmaps, which keep track of which sectors within a band have and have not been allocated. Banding increases performance because the drive head does not have to return to the logical top (typically cylinder 0) of the disk, but to the nearest band allocation bitmap to determine where a file is to be stored.

Additionally, HPFS includes a couple of unique special data objects:

Super Block

The Super Block is located in logical sector 16 and contains a pointer to the FNODE of the root directory. One of the biggest dangers of using HPFS is that if the Super Block is lost or corrupted due to a bad sector, so are the contents of the partition, even if the rest of the drive is fine. It would be possible to recover the data on the drive by copying everything to another drive with a good sector 16 and rebuilding the Super Block. However, this is a very complex task.

Spare Block

The Spare Block is located in logical sector 17 and contains a table of "hot fixes" and the Spare Directory Block. Under HPFS, when a bad sector is detected, the "hot fixes" entry is used to logically point to an existing good sector in place of the bad sector. This technique for handling write errors is known as hot fixing.

Hot fixing is a technique where if an error occurs because of a bad sector, the file system moves the information to a different sector and marks the original sector as bad. This is all done transparent to any applications that are performing disk I/O (that is, the application never knows that there were any problems with the hard drive). Using a file system that supports hot fixing will eliminate error messages such as the FAT "Abort, Retry, or Fail?" error message that occurs when a bad sector is encountered.

> ⓘ **Note**
>
> The version of HPFS that is included with Windows NT does not support hot fixing.

Advantages of HPFS

HPFS is best for drives in the 200-400 MB range. For more discussion of the advantages of HPFS, see the following:

- Windows NT Server "Concepts and Planning Guide," Chapter 5, section titled "Choosing a File System"
- Windows NT Workstation 4.0 Resource Kit, Chapter 18, "Choosing a File System"
- Windows NT Server 4.0 Resource Kit "Resource Guide," Chapter 3, section titled "Which File System to Use on Which Volumes"

Disadvantages of HPFS

Because of the overhead involved in HPFS, it is not a very efficient choice for a volume of under approximately 200 MB. In addition, with volumes larger than about 400 MB, there will be some performance degradation. You cannot set security on HPFS under Windows NT.

HPFS is only supported under Windows NT versions 3.1, 3.5, and 3.51. Windows NT 4.0 cannot access HPFS partitions.

For additional disadvantages of HPFS, see the following:

- Windows NT Server "Concepts and Planning Guide," Chapter 5, section titled "Choosing a File System"
- Windows NT Workstation 4.0 Resource Kit, Chapter 18, "Choosing a File System"
- Windows NT Server 4.0 Resource Kit "Resource Guide," Chapter 3, section titled "Which File System to Use on Which Volumes"

NTFS overview

From a user's point of view, NTFS continues to organize files into directories, which, like HPFS, are sorted. However, unlike FAT or HPFS, there are no "special" objects on the disk and there is no dependence on the underlying hardware, such as 512-byte sectors. In addition, there are no special locations on the disk, such as FAT tables or HPFS Super Blocks.

The goals of NTFS are to provide:

- Reliability, which is especially desirable for high end systems and file servers
- A platform for added functionality
- Support POSIX requirements
- Removal of the limitations of the FAT and HPFS file systems

Reliability

To ensure reliability of NTFS, three major areas were addressed: recoverability, removal of fatal single sector failures, and hot fixing.

NTFS is a recoverable file system because it keeps track of transactions against the file system. When a CHKDSK is performed on FAT or HPFS, the consistency of pointers within the directory, allocation, and file tables are being checked. Under NTFS, a log of

transactions against these components is maintained so that CHKDSK need only roll back transactions to the last commit point in order to recover consistency within the file system.

Under FAT or HPFS, if a sector that is the location of one of the file system's special objects fails, then a single sector failure will occur. NTFS avoids this in two ways: first, by not using special objects on the disk and tracking and protecting all objects that are on the disk. Secondly, under NTFS, multiple copies (the number depends on the volume size) of the Master File Table are kept.

Similar to OS/2 versions of HPFS, NTFS supports hot fixing.

Added functionality

One of the major design goals of Windows NT at every level is to provide a platform that can be added to and built upon, and NTFS is no exception. NTFS provides a rich and flexible platform for other file systems to be able to use. In addition, NTFS fully supports the Windows NT security model and supports multiple data streams. No longer is a data file a single stream of data. Finally, under NTFS, a user can add his or her own user-defined attributes to a file.

POSIX support

NTFS is the most POSIX.1 compliant of the supported file systems because it supports the following POSIX.1 requirements:

Case-sensitive naming:

Under POSIX, README.TXT, Readme.txt, and readme.txt are all different files.

Additional time stamp:

The additional time stamp supplies the time at which the file was last accessed.

Hard links:

A hard link is when two different filenames, which can be located in different directories, point to the same data.

Remove limitations

First, NTFS has greatly increased the size of files and volumes, so that they can now be up to 2^64 bytes (16 exabytes or 18,446,744,073,709,551,616 bytes). NTFS has also

returned to the FAT concept of clusters in order to avoid HPFS problem of a fixed sector size. This was done because Windows NT is a portable operating system and different disk technology is likely to be encountered at some point. Therefore, 512 bytes per sector was viewed as having a large possibility of not always being a good fit for the allocation. This was accomplished by allowing the cluster to be defined as multiples of the hardware's natural allocation size. Finally, in NTFS all filenames are Unicode based, and 8.3 filenames are kept along with long filenames.

Advantages of NTFS

NTFS is best for use on volumes of about 400 MB or more. This is because performance does not degrade under NTFS, as it does under FAT, with larger volume sizes.

The recoverability designed into NTFS is such that a user should never have to run any sort of disk repair utility on an NTFS partition. For additional advantages of NTFS, see the following:

- Windows NT Server "Concepts and Planning Guide," Chapter 5, section titled "Choosing a File System"
- Windows NT Workstation 4.0 Resource Kit, Chapter 18, "Choosing a File System"
- Windows NT Server 4.0 Resource Kit "Resource Guide," Chapter 3, section titled "Which File System to Use on Which Volumes"

Disadvantages of NTFS

It is not recommended to use NTFS on a volume that is smaller than approximately 400 MB, because of the amount of space overhead involved in NTFS. This space overhead is in the form of NTFS system files that typically use at least 4 MB of drive space on a 100-MB partition.

Currently, there is no file encryption built into NTFS. Therefore, someone can boot under MS-DOS, or another operating system, and use a low-level disk editing utility to view data stored on an NTFS volume.

It is not possible to format a floppy disk with the NTFS file system; Windows NT formats all floppy disks with the FAT file system because the overhead involved in NTFS will not fit onto a floppy disk.

For further discussion of NTFS disadvantages, see the following:

- Windows NT Server "Concepts and Planning Guide," Chapter 5, section titled "Choosing a File System"
- Windows NT Workstation 4.0 Resource Kit, Chapter 18, "Choosing a File System"
- Windows NT Server 4.0 Resource Kit "Resource Guide," Chapter 3, section titled "Which File System to Use on Which Volumes"

NTFS naming conventions

File and directory names can be up to 255 characters long, including any extensions. Names preserve case, but are not case-sensitive. NTFS makes no distinction of filenames based on case. Names can contain any characters except for the following:

```
? " / \ < > * | :
```

Currently, from the command line, you can only create file names of up to 253 characters.

> **Note**
>
> Underlying hardware limitations may impose additional partition size limitations in any file system. Particularly, a boot partition can be only 7.8 GB in size, and there is a 2-terabyte limitation in the partition table.

For more information about the supported file systems for Windows NT, see the Windows NT Resource Kit.

Event ID 158 is logged for identical disk GUIDs

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution to solve the event ID 158 that's logged for identical disk GUIDs in Windows 10.

Applies to: Windows 10 - all editions
Original KB number: 2983588

Symptoms

An error event for Event ID 158 is logged. The event indicates that two or more disk devices are assigned identical disk GUIDs.

> ⓘ **Note**
>
> The above event message has no functionality or performance impact on the client systems. This event provides a warning that multiple disks on the system shared the same identification information (like serial number, page 83 IDs, and so on.)

Cause

This problem may be caused by any one of several different situations. The two most common situations are the following ones:

- Multiple paths to the same physical disk device are available. But Microsoft Multipath I/O (MPIO) isn't enabled. In this situation, the device is exposed to the system by all paths that are available. It causes the same device ID data (such as Device Serial Number, Vendor ID, Product ID, and so on) to be exposed multiple times.
- If Virtual Hard Disks (VHD) are duplicated by using a copy-and-paste operation to create more virtual machines (VMs), none of the internal data structures are changed. So, the VMs have the same disk GUIDs and the same ID information (such as Device Serial Number, Vendor ID, Product ID, and so on).

Resolution

To resolve this problem, if multiple paths are available to the physical disk devices, enable MPIO. If MPIO is enabled, the system can claim the drives and expose only one instance of each disk device when the computer is restarted.

More Information

For more information about how to enable MPIO, see Installing and Configuring MPIO.

If multiple VHDs are identified as duplicates, use the `ResetDiskIdentifier` parameter of the `Set-VHD` Windows PowerShell cmdlet. For more information about the `Set-VHD` cmdlet, see Set-VHD.

Garmin USB devices don't work with Windows 10

Article • 09/23/2021 • 2 minutes to read

This article provides information on how to fix the problem that Garmin wearable devices aren't recognized on Windows 10.

Applies to: Windows 10, version 1709, Windows 10, version 1607
Original KB number: 3183365

Symptoms

After you upgrade a computer or device to Windows 10, certain Garmin wearable devices may not work as expected when they're connected to a USB port.

Although the Garmin device shows up in Device Manager and is displayed as a connected drive in File Explorer, it isn't accessible. Attempts to access the drive trigger errors such as the following ones:

> Please insert a disk.

> The directory name is invalid.

Cause

This problem occurs because Garmin devices formatted with FAT12, FAT16, or FAT32 file systems aren't recognized as mass storage devices by a computer or device that's running Windows 10.

Resolution

To resolve the issue, download and install the latest version of Garmin Express software. The Garmin Express tool recognizes the connected device and updates its boot code to make it compatible with Windows 10.

This issue is documented by Garmin at the following site:

Device is not detected in Windows 10 after updating to the Anniversary update.

To download the latest Garmin Express tool, go to Garmin Express.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

How to use System Restore to log on when you lose access to an account

Article • 09/23/2021 • 3 minutes to read

This article provides some information about how to use System Restore to log on when you lose access to an account.

Applies to: Windows 7 Service Pack 1
Original KB number: 940765

> **Note**

Support for Windows Vista without any service packs installed ended on April 13, 2010. To continue receiving security updates for Windows, make sure you're running Windows Vista with Service Pack 2 (SP2). For more information, visit this Microsoft web page: Support is ending for some versions of Windows

Introduction

This article describes how to use the System Restore feature to log on to Windows 7 or Windows Vista when you lose access to an account.

More information

If you cannot log on to Windows 7 or Windows Vista, you can use the Windows Vista System Restore feature, or the Windows 7 System Restore feature.

You may be unable to log on to Windows Vista or Windows 7 in the following scenarios:

- Scenario 1: You recently set a new password for the protected administrator account. However, you don't remember the password.
- Scenario 2: You type the correct logon password. However, Windows Vista or Windows 7 does not accept the password because the system is corrupted.
- Scenario 3: You delete a protected administrator account. Now, you can't log on to another administrator account.
- Scenario 4: You change a protected administrator account to a standard user account. Now, you can't log on to another administrator account.

To use System Restore to log on to Windows Vista or Windows 7 when you lose access to an account, follow these steps.

> ⓘ **Note**
>
> To do this, there must be a System Restore point at which the logon was successful.

1. Insert the Windows Vista or Windows 7 DVD, and then restart the computer.
2. When you receive the following message, press any key: Press any key to boot from CD or DVD.
3. Set the following preferences, and then click **Next:
   - **Language to install**
   - **Time and currency format**
   - **Keyboard or input method**
4. Click **Repair your computer**, select the operating system that you want to repair, and then click **Next**.
5. Click **System Restore**, and then click **Next**.
6. Click the restore point that you want to use, and then click **Next**.

   > ⓘ **Note**
   >
   > Click a restore point that will return the computer to a state where the logon is successful. After you use the System Restore feature, reinstall any programs or updates that may be removed. You will not lose any personal documents. However, you may have to reinstall programs. You may also have to reset some personal settings.
7. Confirm the disks that you want to restore, and then click **Next**.
8. Click **Finish**, and then click **Yes** for the prompt box.
9. When the System Restore process is complete, click **Restart** to restart the computer.
10. After the computer restarts, click **Close** to confirm that the System Restore process has finished successfully.

11. Use an appropriate method to log on. For example, log on by using an older password, or log on by using another computer account. After you log on, you must follow additional steps, depending on the scenario that you experience.

Additional steps for scenario 1

1. After you log on, change the password for the protected administrator account.
2. After you change the password, restart the computer. Make sure that you can log on by using the new password.

Additional steps for scenario 2

1. After you log on, make sure that each user account can log on by using the appropriate credentials.
2. Change the password for the user account that cannot log on.

Additional steps for scenario 3

1. After you log on, use the User Accounts item in Control Panel to create a new protected administrator account.
2. Log on by using the new protected administrator account. Then, delete the older protected administrator account that was restored.

> **Note**
>
> For safety reasons, do not use the restored protected administrator account.

Additional steps for scenario 4

1. After you log on, use the User Accounts item in Control Panel to create a new protected administrator account.
2. Log on by using the new protected administrator account.
3. Change the old protected administrator account to a standard user account.

System Restore may fail with error code 0x8007045b if there is encrypted content in the restore point

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where System Restore may fail with error code 0x8007045b.

Applies to: Windows 10 - all editions
Original KB number: 3074925

Symptoms

Consider the following scenario:

- You are using the Mail application in Windows 8.1 or Windows 8.
- You want to use the Mail application to connect to a Microsoft Exchange or Microsoft Office 365 mail server. (To do this, you have to accept the **Make my PC more secure** security policies that are applied from the mail server.)
- You take one of the following actions:
  - You use the System Restore program in Windows to create some restore points.
  - You try to use restore points that were created by the system automatically.
- You try to restore the system back to one of the restore points after you accept enforced security.

In this scenario, System Restore may fail, and you receive an error message that resembles the following after the system is restarted.

> System Restore did not complete successfully. Your computer's system files and settings were not changed.
>
> Details:
>
> System Restore failed to extract the file
>
> C:\Users< **User Name** >\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe....
>
> From the restore point.

> An unexpected error occurred during System Restore. (0x8007045b)

Cause

This problem occurs because of a known issue in the System Restore program.

After you configure the Mail application to connect to an Exchange or Office 365 server and accept the **Make my PC more secure** security policies, some files in the user profile will be encrypted by using the Encrypting File System (EFS). And those files will be included in the restore point if you use System Restore to create a restore point. When you start the System Restore program to restore the system, System Restore creates a shutdown task to do the real restoration work. When this task is being executed, most system services are already stopped. This includes EFS.

However, if any file is being encrypted by EFS in the restore point, the System Restore program will have to call in to the EFS service to extract files of this kind from the restore point. But because the EFS service is already stopped and cannot be restarted because the system is being shutting down, the restoration process fails with error code 0x8007045b. This code means ERROR_SHUTDOWN_IN_PROGRESS.

Workaround

To work around this issue, follow these steps to restart into Windows RE, and then run the System Restore program.

1. Open a command prompt as Administrator, and then run the following command:

   ```
   Console

   reagentc /boottore
   ```

   > **Note**
   >
   > If this command returns a **Windows RE is disabled** error, run the following command to install it, and then run `reagentc /enable` again.

2. Restart the computer. The computer will restart into the Windows RE environment.

3. In Windows RE, click **Troubleshoot**, click **Advanced Options**, click **System Restore**, and then follow the prompt to start the System Restore program. Because EFS is always running in Windows RE, and because System Restore doesn't have to create

a shutdown task to perform the restoration work in Windows RE, this specific issue will not occur in Windows RE. For more information about the REAgentC command, see REAgentC Command-Line Options.

e2e: Event IDs for Volsnap

Article • 12/06/2021 • 2 minutes to read

This article provides some information about Event IDs for Volsnap.

Applies to: Windows 10 - all editions
Original KB number: 3081408

Summary

In Windows 10, Volsnap has Event Tracing for Windows (ETW) tracing and flexible event logging. These features may be useful in the following scenarios:

- Recording statistics about mounting. For example, when you encounter an issue in which bringing a volume online takes a long time, Volsnap frequently is implicated in the delay. Decent diagnostic information will be helpful in troubleshooting.
- Debugging or diagnosis of snapshot failures, especially in scenarios in which it is difficult to use the debugger.

The features also play into a larger effort to provide diagnosability in the storage stack for complex operations such as cluster online/offline and for end-to-end diagnostics of storage stack failures.

The new diagnostics consist of a set of new ETW events that are logged to the Operational channel. The operational channel receives low-volume events that describe important events during infrequent large operations, such as volume online, volume offline, and so on.

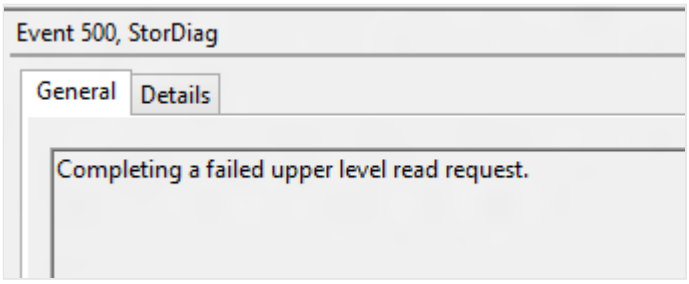
In Windows 10, Volsnap also changes the way it logs to the System log. The legacy `IoWriteErrorLogEntry` API is no longer used. Instead, Volsnap imports the System log as an ETW channel and redefines its current complement of System events to provide richer information, as required.

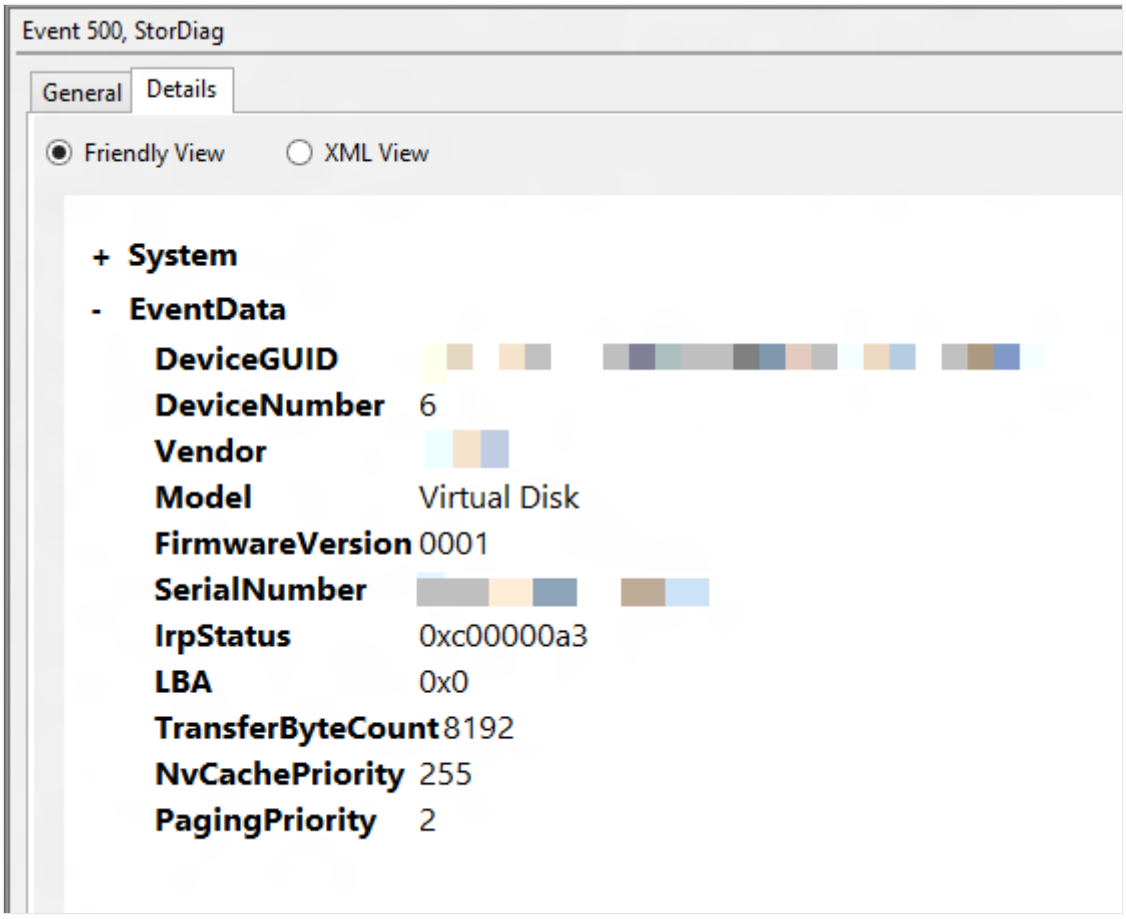
Finally, Volsnap supports the acquisition and transfer of activity IDs.

Possible events for Volsnap

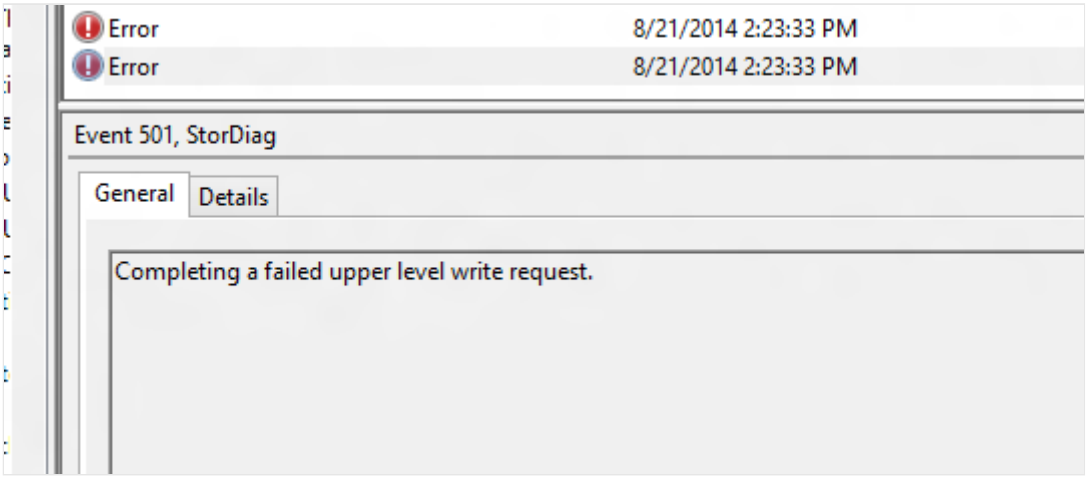
For the Operational channel, the following are all the possible events.

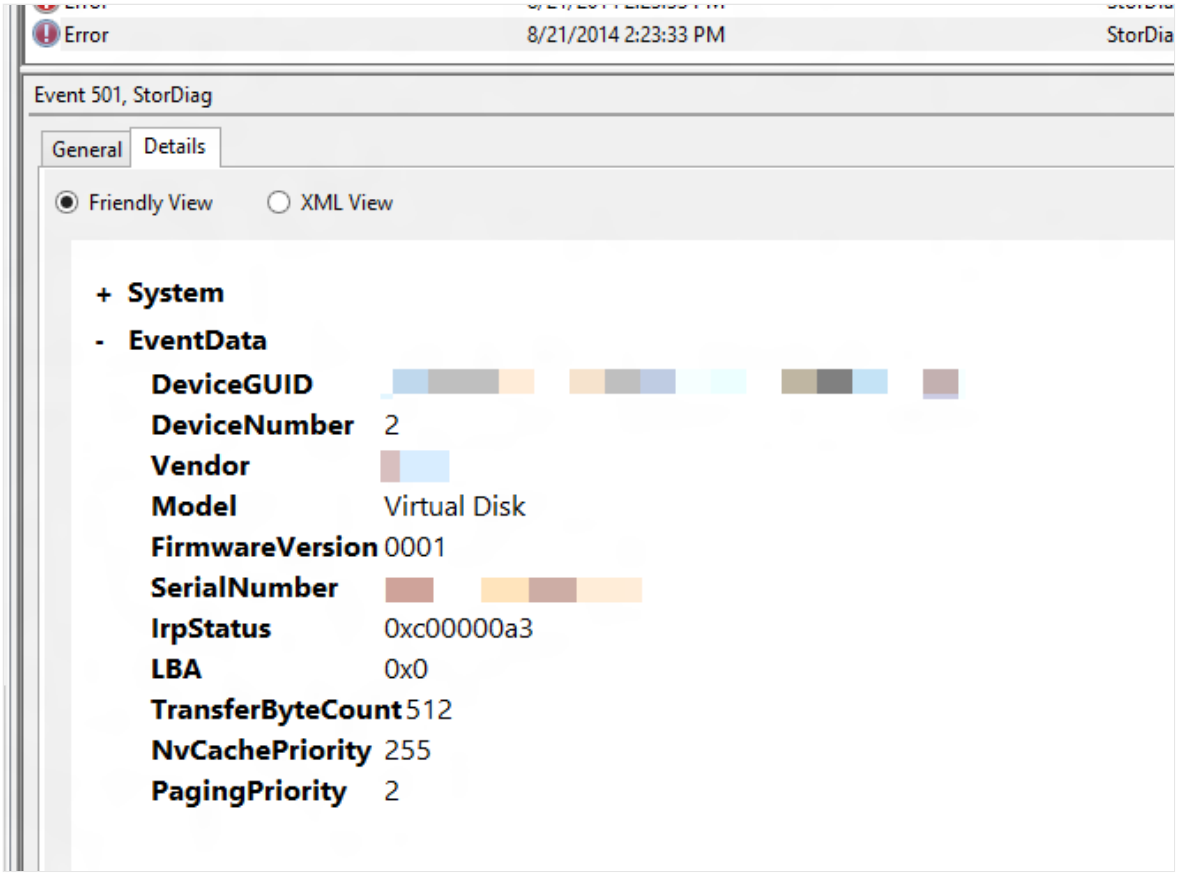
- 500 Completing a failed upper-level read request



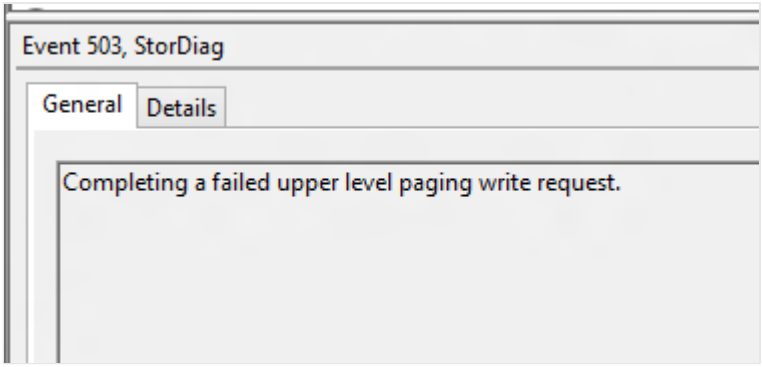


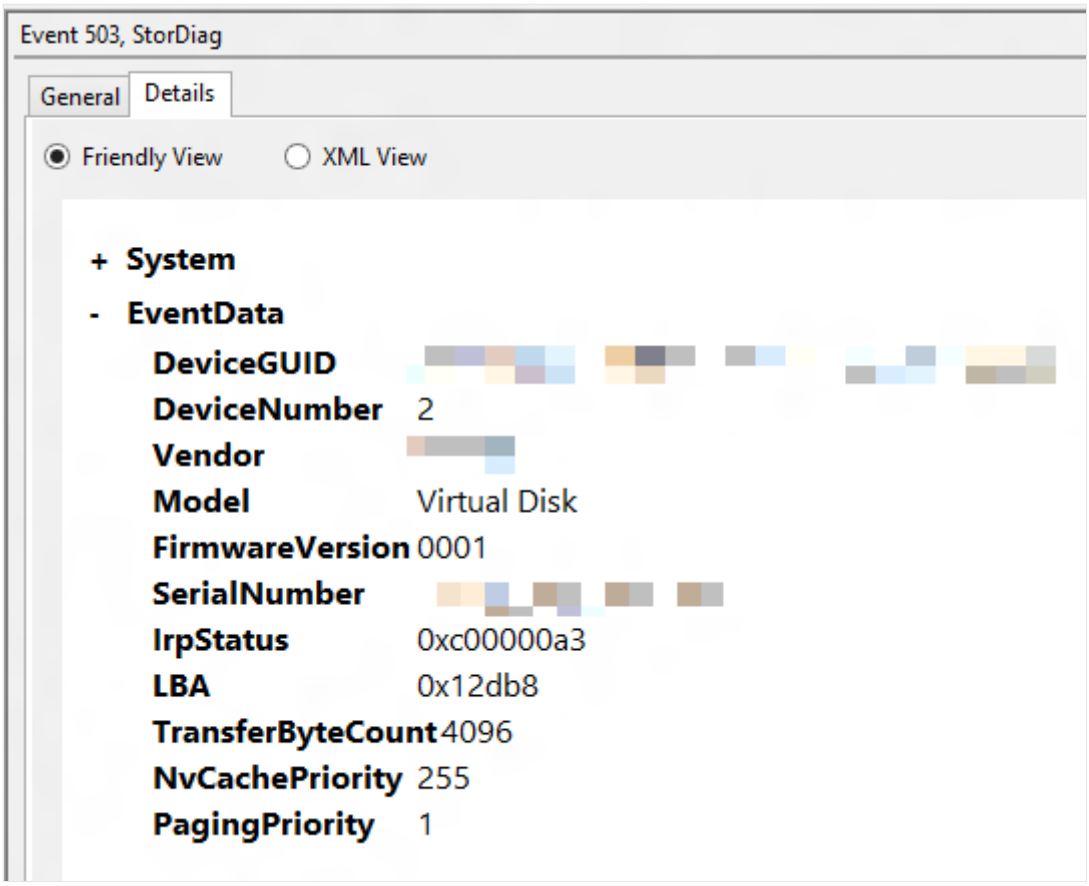
- 501 Completing a failed upper-level write request



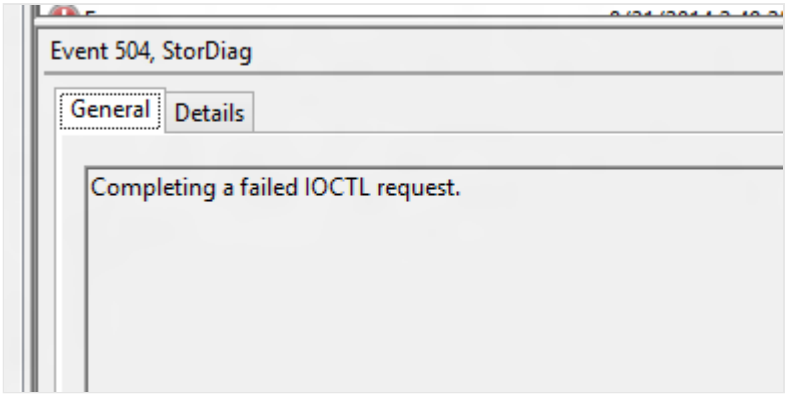


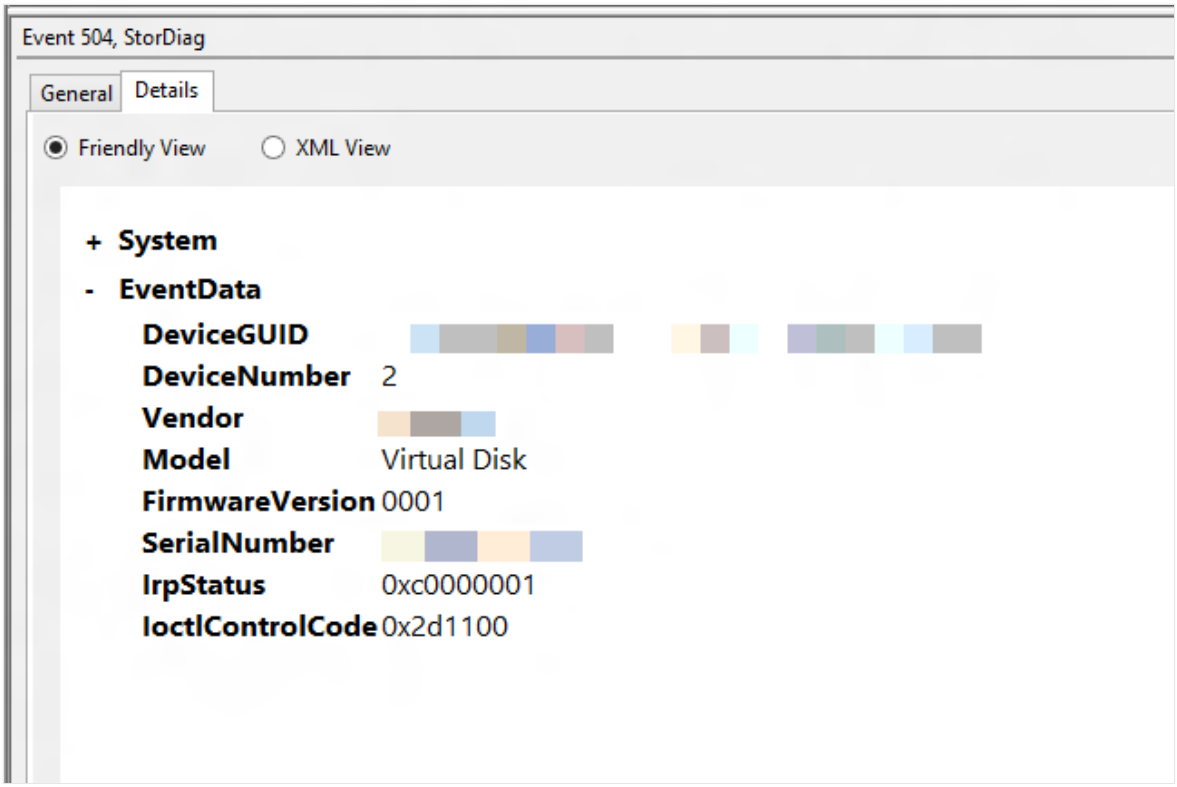
- 503 Completing a failed upper-level paging write request



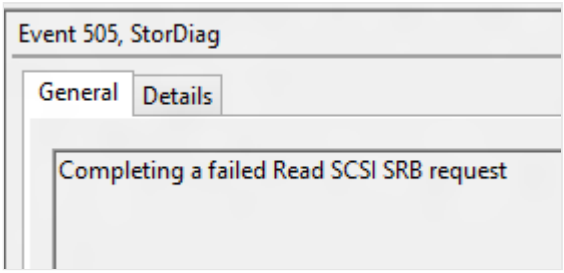


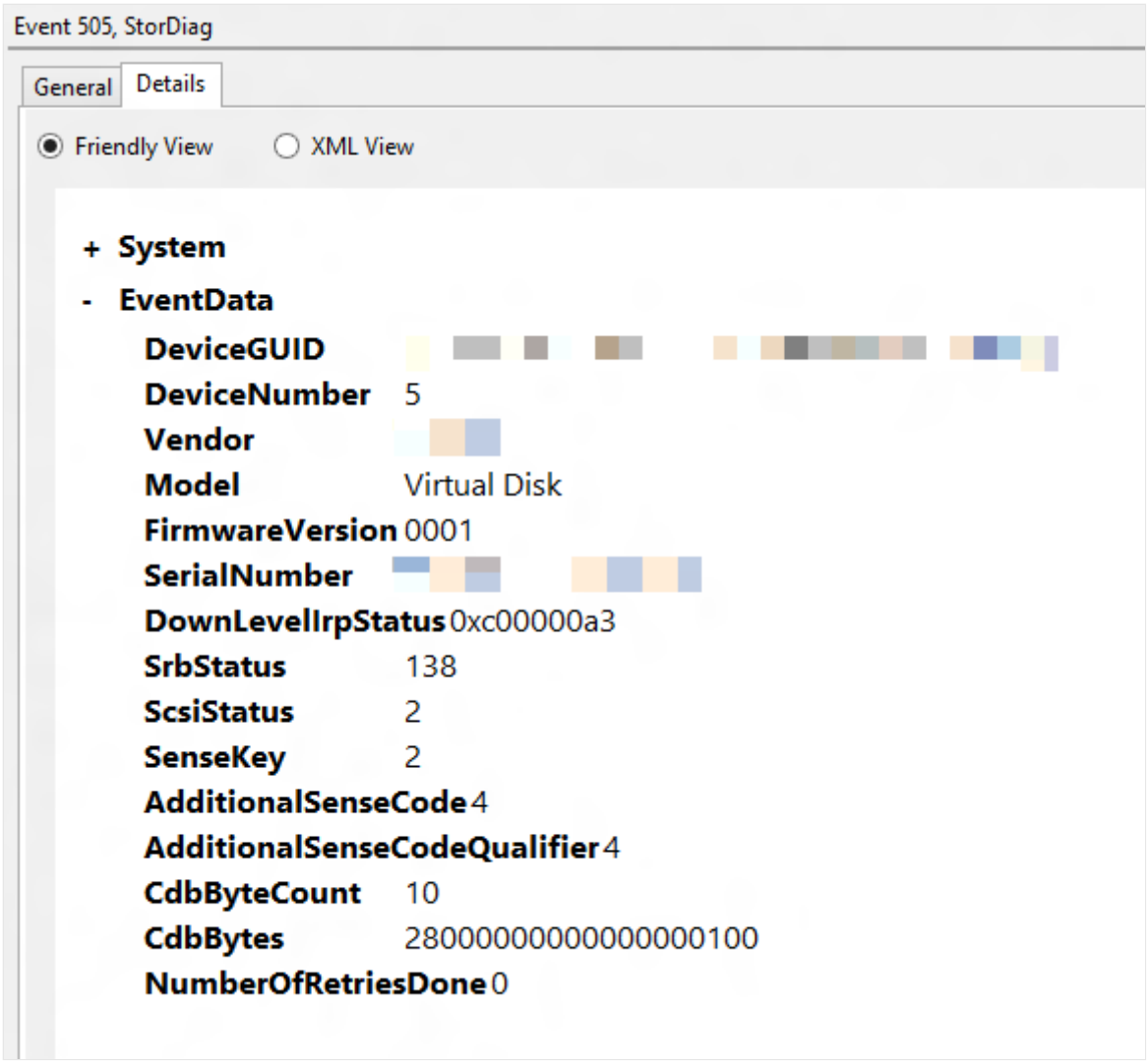
- 504 Completing a failed IOCTL request



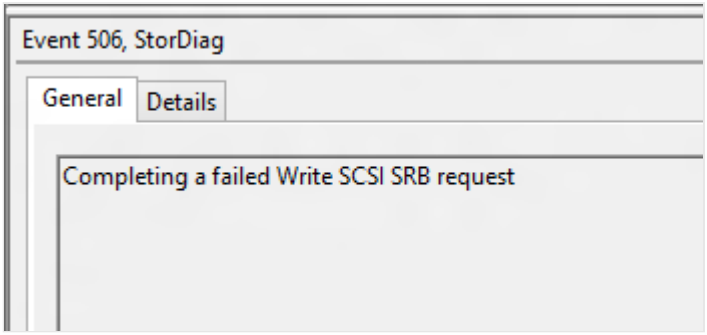


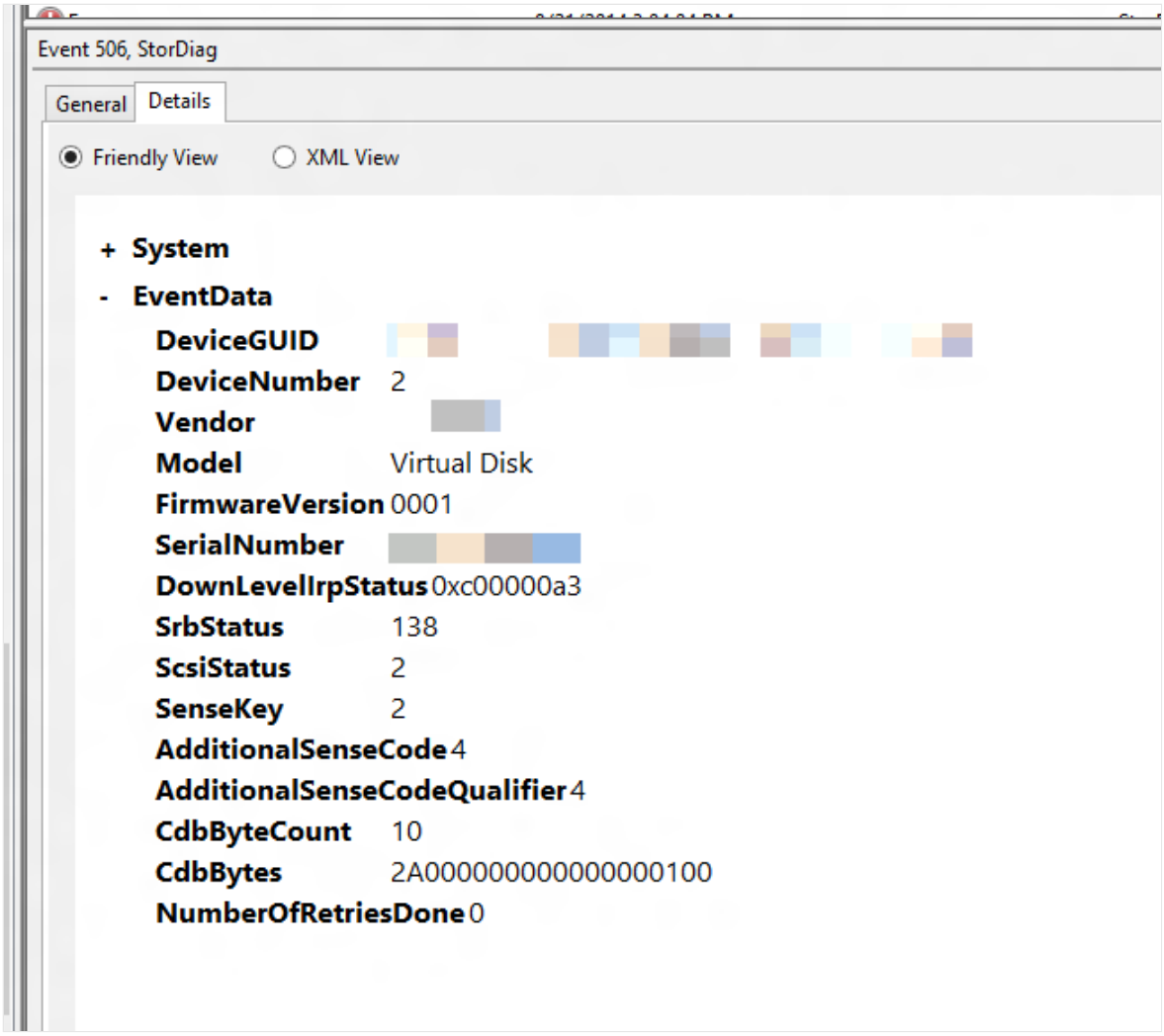
- 505 Completing a failed Read SCSI SRB request



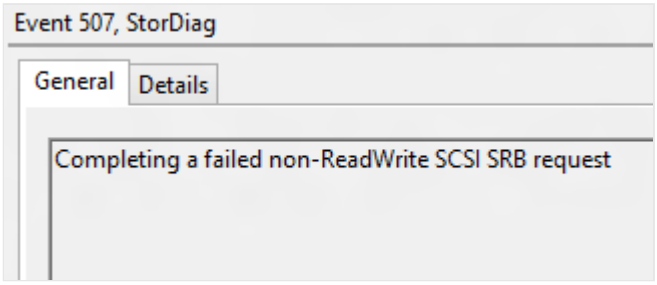


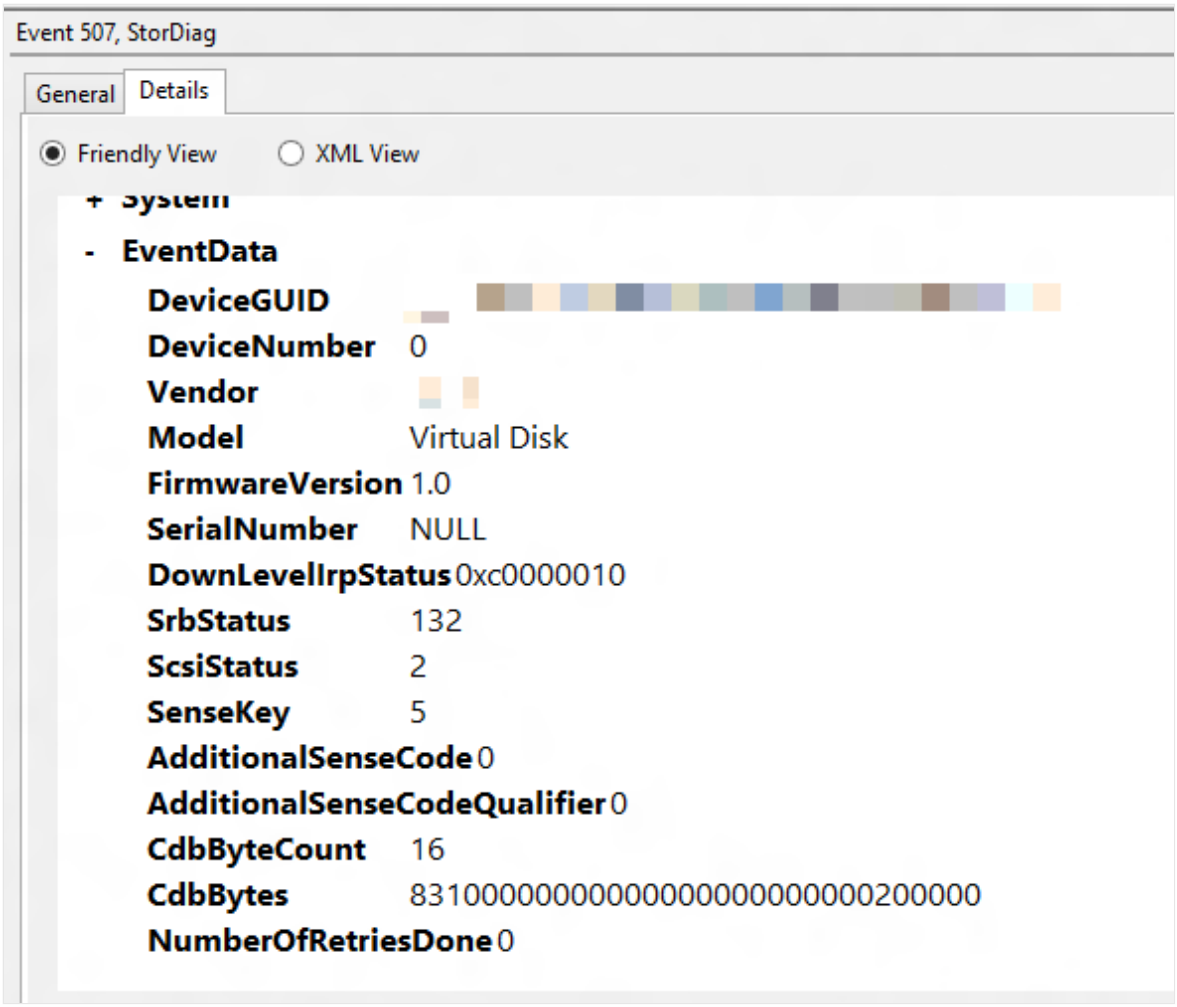
- 506 Completing a failed Write SCSI SRB request



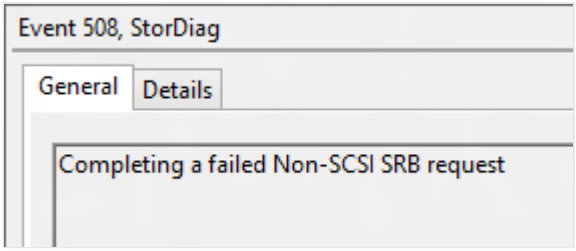


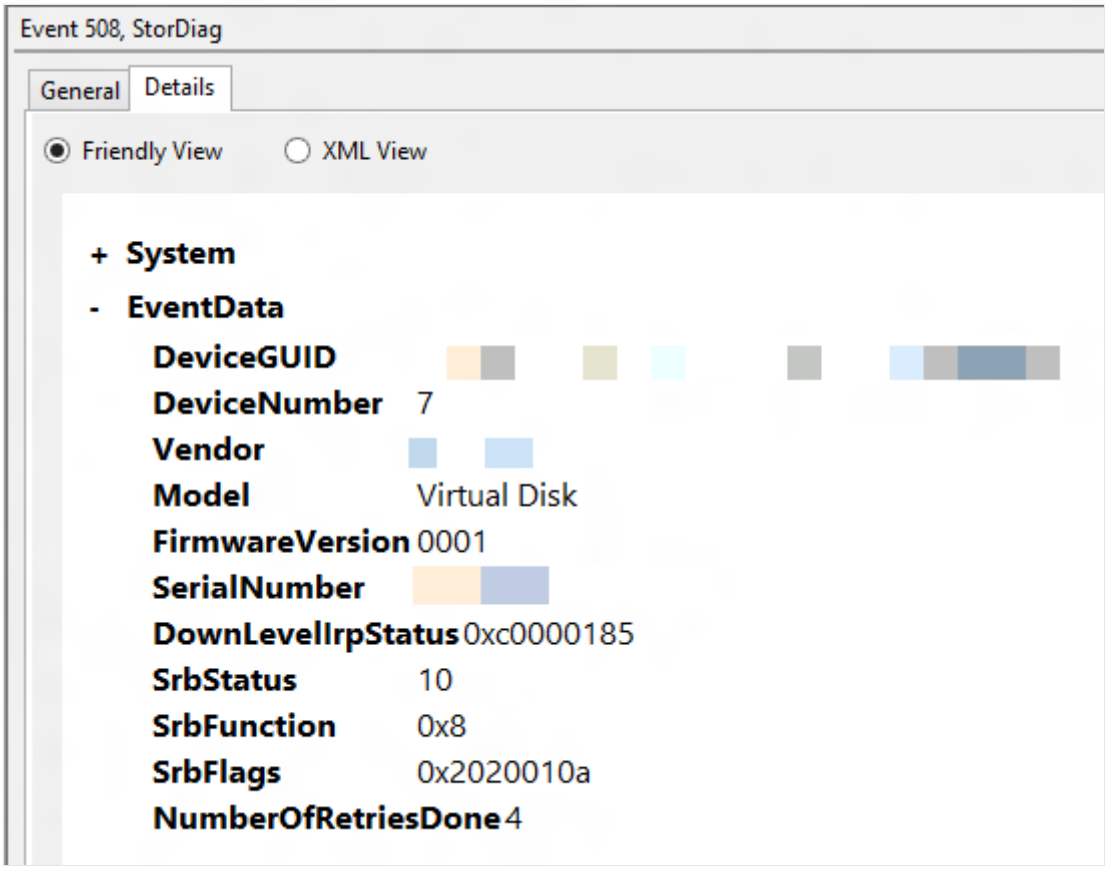
- 507 Completing a failed non-ReadWrite SCSI SRB request



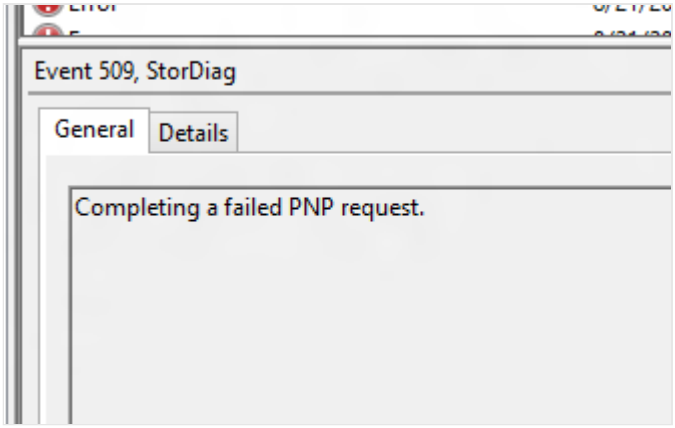


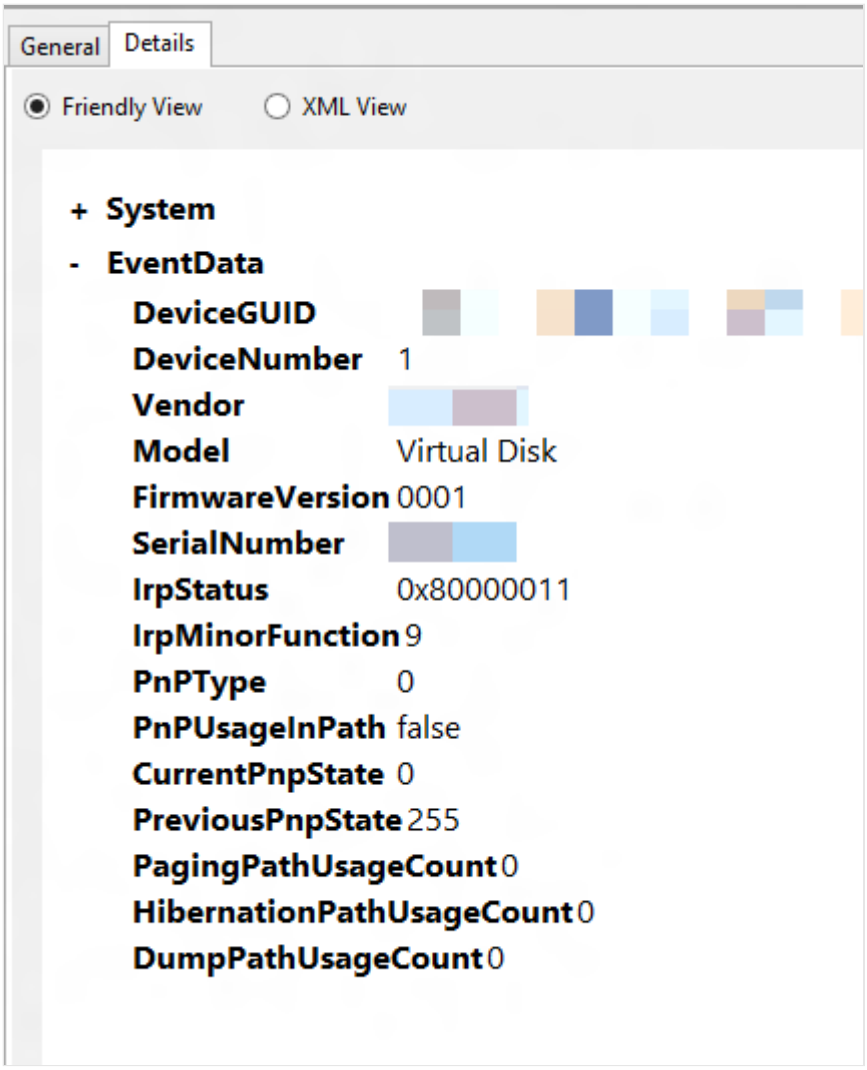
- 508 Completing a failed non-SCSI SRB request



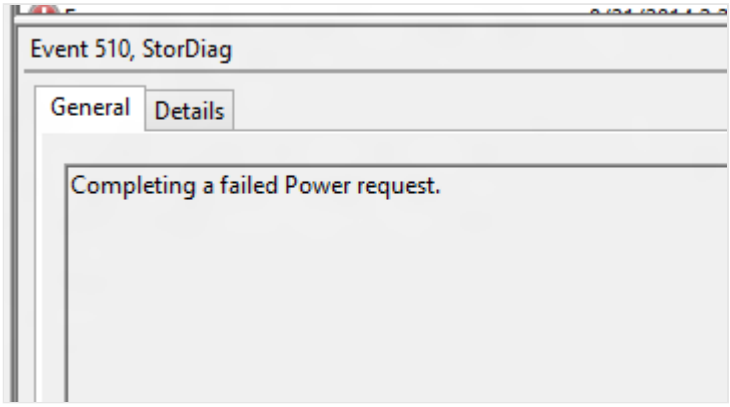


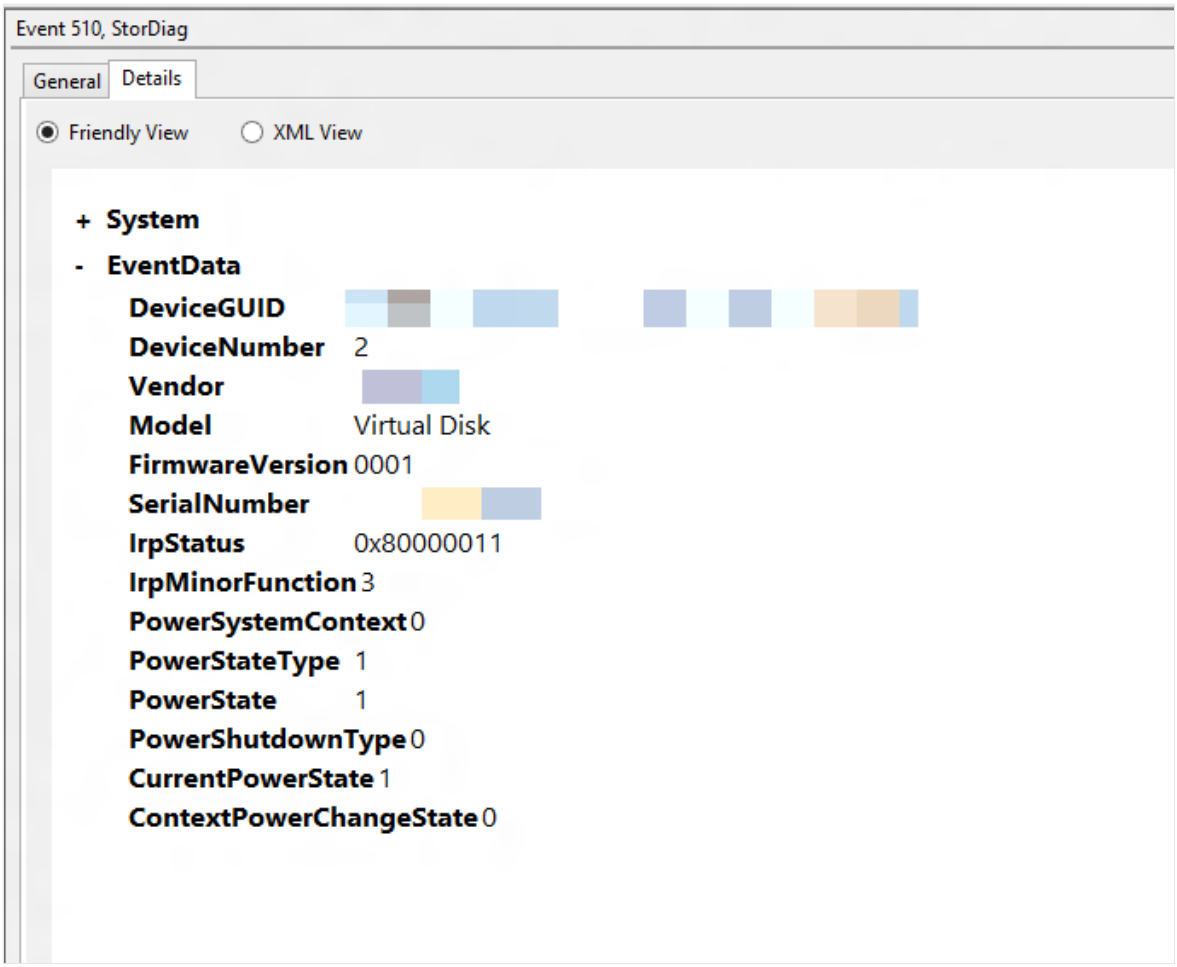
- 509 Completing a failed PNP request





- 510 Completing a failed Power request

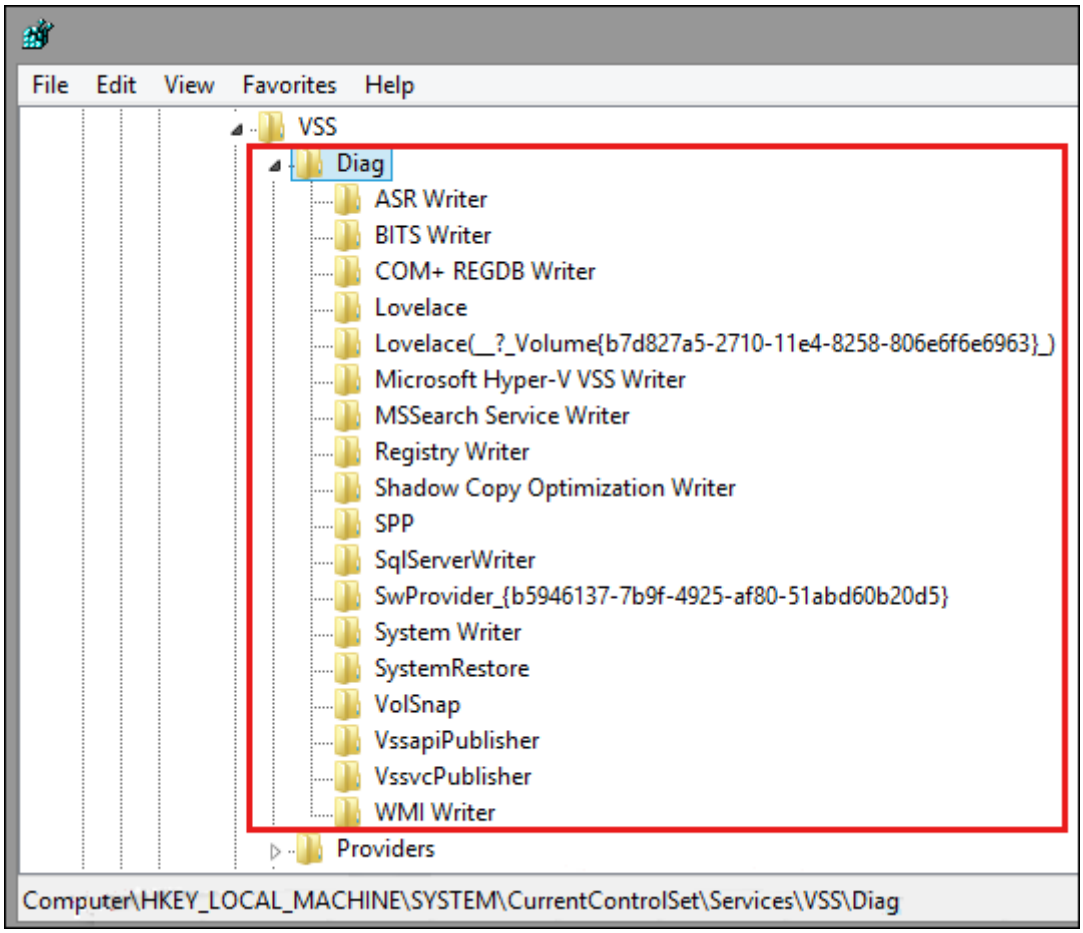




- 511 Completing a failed WMI request

In earlier versions of Windows

In earlier versions of Windows, Volsnap had limited diagnostic features. Although it can log 42 different event messages, the routines that produce them are limited to providing up to two strings that represent volume names. The messages were logged by using the older API `IoWriteErrorLogEntry`. There was also a custom logging facility that was shared between Volsnap and various other components of VSS. In this custom logging, diagnostic data was written to the registry under `HKEY_LOCAL_MACHINE\SYSTEM\CCS\Services\vss\Diag`.



This mechanism was specific to the Volume Shadow Copy Service (VSS). Therefore, it required custom tools, such as VSS Reports, to extract the information. Also, it retained only the most recent instance of any given diagnostic message.

> ⓘ **Note**
>
> The legacy method of VSS logging is still used in Windows 10 because the ETW addition does not provide a complete replacement.

Most recent previous versions are missing for a share that has Previous Versions enabled in Windows

Article • 04/29/2022 • 2 minutes to read

This article provides a workaround for an issue in which most recent previous versions aren't displayed for a share in Windows that has the **Previous Versions** feature enabled.

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 4032986

Symptoms

You've modified the **MaxShadowCopies** registry value to a larger value (the default value is 64). The **MaxShadowCopies** registry value specifies the maximum number of snapshots which the Volume Shadow Copy Service (VSS) can retain. When you connect to a share that has the **Previous Versions** feature enabled, you can see only older previous versions. The most recent previous versions are missing for the share.

Cause

This issue occurs because the VSS and the Server Message Block (SMB) server components have separate limit numbers. The VSS limit number can be modified by the registry, but the SMB server has a fixed limit number that varies in Windows versions. Windows 8, Windows Server 2012, and later Windows versions are limited to view 500 previous versions in the SMB server. If you set the **MaxShadowCopies** registry value to 512, only the oldest 500 previous versions are displayed on the client side. Therefore, you can't see the 12 most recent previous versions.

Workaround

To work around this issue, limit the number of previous versions that are kept on the server to 500 per volume.

More Information

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

By default, Windows keeps only 64 snapshots per volume for previous versions. You can adjust this limit by creating or changing the following registry key:
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VSS\Settings\MaxShadowCopies`

See Registry Keys and Values for Backup and Restore for more information.

Setting this key to a value higher than the SMB server can handle prevents users from seeing the most recent previous versions. The SMB server's limit for each operating system is as follows:

- Windows 8, Windows Server 2012, and later versions have a limit of 500.
- Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2 have a limit of 500 for the SMB version 1 (SMBv1) protocol and 64 for the SMB version 2 (SMBv2) protocol.
- Windows XP and Windows Server 2003 have a limit of 64.

> **Note**
>
> The SMB server's limit isn't adjustable. You can only modify the **MaxShadowCopies** registry value to adjust the number of previous versions that are kept.

Deployment troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Deployment-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Deployment sub categories

- Activation
- Bitlocker
- Devices and Drivers
- Power Management
- Servicing
- Setup

Activation failures and (not genuine) notifications around January 8, 2019, on volume-licensed Windows 7 Service Pack 1 KMS clients

Article • 03/24/2022 • 4 minutes to read

This article provides a solution to an issue where users may receive the Windows Activation or "Windows is not genuine" notifications starting at or after 10:00 UTC, January 8, 2019.

Applies to: Windows 7 Service Pack 1
Original KB number: 4487266

Summary

This article applies to volume-licensed Windows 7 Service Pack 1 devices that use Key Management Service (KMS) activation and have the KB 971033 update installed. Some users may receive the Windows Activation or "Windows is not genuine" notifications starting at or after 10:00 UTC, January 8, 2019.

On January 9, 2019, we reverted a change that was made to Microsoft Activation and Validation servers. For devices that continue to report activation and "not genuine" notifications, you should remove KB 971033 by following the steps in the Resolution section.

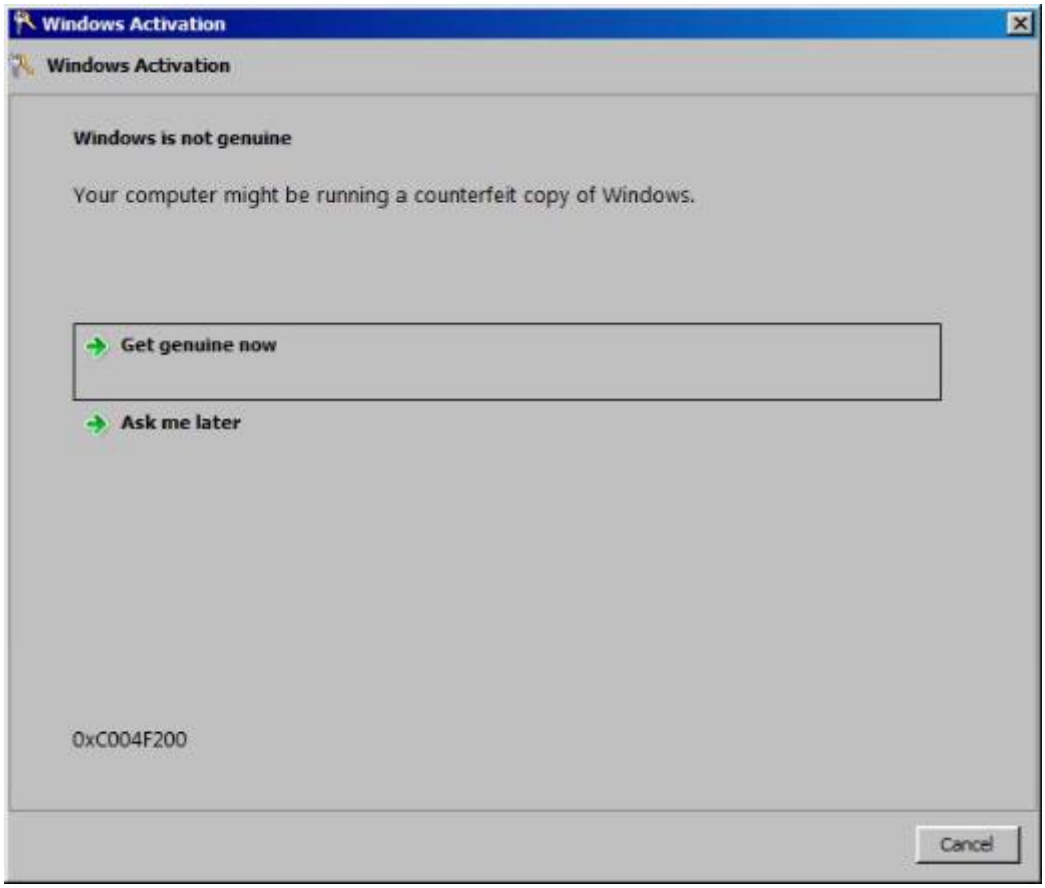
Windows editions that support volume-licensing activation include the following:

- Windows 7 Professional
- Windows 7 Professional N
- Windows 7 Professional E
- Windows 7 Enterprise
- Windows 7 Enterprise N
- Windows 7 Enterprise E

For Windows editions that experience activation and "not genuine" errors that are not caused by the Microsoft Activation and Validation server change around January 8, 2019, we recommend that you follow standard activation troubleshooting.

Symptoms

1. You receive a **Windows is not genuine** error message after you log on.



2. A **This copy of windows is not genuine** watermark appears in the bottom-right corner of the Windows desktop on a black background.



3. The `slmgr /dlv` output reports error 0xC004F200.

```
Software licensing service version: 6.1.7601.17514

Name: Windows(R) 7, Enterprise edition
Description: Windows Operating System - Windows(R) 7, VOLUME_KMSCLIENT channel
Activation ID: [redacted]
Application ID: [redacted]
Extended PID:
Installation ID:
Partial Product Key: H[redacted]
License Status: Notification
Notification Reason: 0xC004F200 (non-genuine).
Remaining Windows rearm count: 2
Trusted time:
Please use slmgr.vbs /ato to activate and update KMS client information in order
 to update values.
```

4. Activations that are made by using the `slmgr /ato` command fails and return the following message:

   > Windows is running within the non-genuine notification period. Run 'slui.exe' to go online and validate Windows.



5. The following events are logged in the event log.

Event log	Event source	Event ID	Description
Application	Microsoft-Windows-Security-SPP	8209	Genuine state set to non-genuine (0x00000000) for application Id 55c92734-d682-4d71-983e-d6ec3f16059f
Application	Microsoft-Windows-Security-SPP	8208	Acquisition of genuine ticket failed (hr=0xC004C4A2) for template Id 66c92734-d682-4d71-983e-d6ec3f16059f
Application	Windows Activation Technologies	13	Genuine validation result: hrOffline = 0x00000000, hrOnline =0xC004C4A2
Application	Microsoft-Windows-Security-SPP	8196	License Activation Scheduler (sppuinotify.dll) was not able to automatically activate. Error code: 0xC004F200:

Cause

A recent update to the Microsoft Activation and Validation unintentionally caused a "not genuine" error on volume-licensed Windows 7 clients that had KB971033 installed. The change was introduced at 10:00:00 UTC on January 8, 2019, and was reverted at 4:30:00 UTC on January 9, 2019.

> ⓘ **Note**
>
> This timing coincides with the release of the "1B" January 2019 updates (**KB 4480960** and **KB 4480970**) that were released on Tuesday, January 8, 2019. These events are not related.

Windows 7 devices that have KB971033 installed but did not experience this issue between the time of the change (10:00:00 UTC, January 8, 2019) and the time of the reversion of that change (4:30:00 UTC, January 9, 2019) should not experience the issue that is described in this article.

KB971033 contains the following text:

"Note For an Enterprise customer who uses Key Management Service (KMS) or Multiple Activation Key (MAK) volume activation, we generally recommend to NOT install this update in their reference image or already deployed computers. This update is targeted at consumer installs of Windows using RETAIL activation."

We strongly recommend that you uninstall KB971033 from all volume-licensed Windows 7-based devices. This includes devices that are not currently affected by the issue that is mentioned in the Symptoms section.

Resolution

To determine whether KB 971033 is installed, use one of the following methods.

- Open the **Installed Updates** item in Control Panel (**Control Panel** > **Windows Update** > **View update history** > **Installed Updates**), and then look for **Update for Microsoft Windows (KB971033)** in the list.
- Run the following command in a Command Prompt window as administrator, and then look for "Microsoft-Windows-Security-WindowsActivationTechnologies-package~31bf3856ad364e35~amd64~~7.1.7600.16395" in the results:

  Console

  ```
  dism /online /get-packages
  ```

- Run the following command at a command prompt, and then look in the results for an indication that KB 971033 is installed:

  Console

  ```
  wmic qfe where HotFixID="KB971033"
  ```

- Run the following command in Windows PowerShell, and then look in the results for an indication that KB 971033 is installed:

  PowerShell

```
Get-Hotfix -id KB971033
```

If KB 971033 is currently installed, use one of the following methods to remove the update. We recommend that you restart the system after the update is removed.

- In the **Installed Updates** item in Control Panel (**Control Panel** > **Windows Update** > **View update history** > **Installed Updates**), right-click **Update for Microsoft Windows (KB971033)**, and then select **Uninstall**.
- Run the following command in a Command Prompt window as administrator:

```
Console

wusa /uninstall /kb:971033
```

- Run the following command in a Command Prompt window as administrator:

```
Console

dism /online /Remove-Package /PackageName:Microsoft-Windows-Security-
WindowsActivationTechnologies-
Package~31bf3856ad364e35~amd64~~7.1.7600.16395
```

After KB 971033 is uninstalled, or after it no longer appears as installed, rebuild the activation-related files and then reactivate the system by running the following commands in a Command Prompt window as administrator:

```
Console

net stop sppuinotify
sc config sppuinotify start= disabled
net stop sppsvc
del %windir%\system32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-
A289-439d-8115-601632D005A0 /ah
del %windir%\system32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-
A289-439d-8115-601632D005A0 /ah
del
%windir%\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\SoftwarePr
otectionPlatform\tokens.dat
del
%windir%\ServiceProfiles\NetworkService\AppData\Roaming\Microsoft\SoftwarePr
otectionPlatform\cache\cache.dat
net start sppsvc
cscript c:\windows\system32\slmgr.vbs /ipk <edition-specific KMS client key>
cscript c:\windows\system32\slmgr.vbs /ato
sc config sppuinotify start= demand
```

> **Note**
>
> In the first cscript command, replace <edition-specific KMS client key> with the actual key. For more information, see **KMS Client Setup Keys**.

The following table lists the KMS client keys for each edition of Windows 7.

Operating system edition	KMS Client Setup Key
Windows 7 Professional	FJ82H-XT6CR-J8D7P-XQJJ2-GPDD4
Windows 7 Professional N	MRPKT-YTG23-K7D7T-X2JMM-QY7MG
Windows 7 Professional E	W82YF-2Q76Y-63HXB-FGJG9-GF7QX
Windows 7 Enterprise	33PXH-7Y6KF-2VJC9-XBBR8-HVTHH
Windows 7 Enterprise N	YDRBP-3D83W-TY26F-D46B2-XCKRJ
Windows 7 Enterprise E	C29WB-22CC8-VJ326-GHFJW-H9DH4

> **Note**
>
> - Scripts that contain the KMS client setup key must target the corresponding operating system edition.
> - For services that do not have **KB 971033** installed but experience the issue that is mentioned in the **Symptoms** section, you can also rebuild activation-related files and reactivate the system by using the script that is mentioned in the list of reactivation commands.

You receive an error message when you try to activate Windows Vista or Windows 7 on a computer that was obtained from an OEM

Article • 09/23/2021 • 4 minutes to read

This article provides a solution to solve errors that occur when you activate Windows Vista or Windows 7 on a computer that's obtained from an Original Equipment Manufacturer (OEM).

Applies to: Windows 7 Service Pack 1
Original KB number: 942962

Symptoms

When you try to activate Windows Vista or Windows 7 on a computer that was obtained from an OEM, you experience one of the following symptoms.

Symptom 1

You receive one of the following error messages:

Error message 1

> Error Code: Invalid Volume License Key
>
> In order to activate, you need to change your product key to a valid Multiple Activation Key (MAK) or Retail key.
>
> You must have a qualifying operating system license AND a Volume license Windows <**operating system**> upgrade license, or a full license for Windows <**operating system**> through an OEM or from a retail source.
>
> ANY OTHER INSTALLATION OF THIS SOFTWARE IS IN VIOLATION OF YOUR AGREEMENT AND APPLICABLE COPYRIGHT LAW.

Error message 2

> Error Code: 0xC004F059

> Description: The Software Licensing Service reported that a license in the computer BIOS is invalid.

Symptom 2

You receive the following error message:

> Error Code: 0xc004f035
> The Software Licensing Service reported that the computer could not be activated with a Volume license product key. Volume licensed systems require upgrading from a qualified operating system. Please contact your system administrator or use a different type of key.

This behavior occurs when the following conditions are true:

- You are using the Key Management Service (KMS) to perform activation.
- The computer uses an ACPI_SLIC table in the computer BIOS program.

> **Note**
>
> An ACPI_SLIC table is used by an Advanced Configuration and Power Interface (ACPI)-compliant BIOS program to store Software Licensing description information.

Cause

This problem occurs if the KMS server does not find a valid Windows marker in the ACPI_SLIC table in the computer's BIOS program. This problem occurs for one of the following reasons.

Cause 1

You purchased a computer that has a qualifying Windows operating system installed. However, the Windows marker in the ACPI_SLIC table is corrupted.

Cause 2

You purchased a computer that does not have a qualifying Windows operating system installed. In this case, the Windows marker is not present in the ACPI_SLIC table.

Resolution

Windows Volume License is for upgrades only. Before you try to upgrade, you must first purchase an underlying, qualifying, and genuine Windows license. For more information, visit the following Microsoft website:
Legalization licensing solutions
The information on this website includes an easy way to correct improper licensing by using a Get Genuine Agreement. Next, you must change the product key to a Multiple Activation Key (MAK). To do this, contact the Microsoft Volume Licensing Service Center at the following Microsoft website:
Volume Licensing Service Center

More information

The behavior that is mentioned in the "Symptoms" section may occur when the Windows marker is missing from the Software Licensing table or when the Windows marker information is present but corrupted. For more information about Volume Activation 2.0, visit the following Microsoft Web site:
Volume Activation 2.0 Operations Guide
A computer that was obtained from an OEM and that has an ACPI_SLIC table in the system BIOS must have a valid Windows marker in that ACPI_SLIC table if that system includes an OEM license for a Microsoft operating system (Windows XP, Windows Vista, or Windows 7). OEM systems that do not include an OEM Microsoft operating system may include an ACPI_SLIC table that does not include a valid marker file. This Windows marker is important for volume license customers who plan to use Windows Vista or Windows 7 volume license media to reimage or upgrade an OEM system according to the reimaging rights in the volume license agreement.

A computer whose ACPI_SLIC table lacks a valid Windows marker generates an error when you try to activate through KMS when you are using a volume edition of Windows Vista or of Windows 7. You cannot activate such a system by using KMS. This is a compliance check for the use of volume media as per the Volume License Agreement. However, you can activate the system by using a multiple activation key (MAK). (You may not be compliant from a licensing scenario when you use a MAK. Contact your licensing specialist to make sure that you are complaint.) Or, you can use a retail key. Alternatively, if you purchased an OEM system that has Windows Vista or Windows 7 installed and activated, you can contact the OEM for more help. Or, you can purchase a new computer that has a Microsoft Windows operating system and an ACPI_SLIC table that has a valid Windows marker.

The MGADiag tool

The MGADiag tool detects and reports BIOS information. However, the BIOS information for the ACPI_SLIC table does not appear in the graphical user interface output. To see the BIOS information, click the **Windows** tab, click **Copy**, and then paste the output into Notepad or into another text editor. The output will resemble the following example:

> Will not be able to KMS Activate:
>
> OEM Activation 2.0 Data-->
> BIOS valid for OA 2.0: No, invalid SLIC table
> Windows marker version: N/A
> OEMID and OEMTableID Consistent: N/A
>
> Windows Marker not present
> OEM Activation 2.0 Data-->
> BIOS valid for OA 2.0: Yes, but no Windows Marker
> Windows marker version: N/A
> OEMID and OEMTableID Consistent: Yes
>
> Will be able to KMS Activate:
>
> Windows Marker present
> OEM Activation 2.0 Data-->
> BIOS valid for OA 2.0: Yes
> Windows marker version: 0x20001
> OEMID and OEMTableID Consistent: Yes
>
> SLIC table not present
> OEM Activation 2.0 Data-->
> BIOS valid for OA 2.0: Yes, but no SLIC table
> Windows marker version: N/A
> OEMID and OEMTableID Consistent: N/A

Note

The KMS compliance check only applies to Windows 7 and Windows Vista machines running as KMS clients, it does not apply to Windows Server 2008 or Windows Server 2008 R2 machines running as KMS client machines.

"An item with the same key has already been added" error when you open a list in VAMT 2.0 on a Windows 7-based computer

Article • 09/23/2021 • 2 minutes to read

This article helps fix an error (An item with the same key has already been added) that occurs when you open a list in Volume Activation Management Tool (VAMT) 2.0.

Applies to: Windows 7 Service Pack 1
Original KB number: 2383895

Symptoms

When you open a list (`.cil`) in VAMT 2.0 on a Windows 7-based computer, you may receive the following error message:

An item with the same key has already been added.

Cause

This problem may occur if there are multiple network adapters in the computer, and these networks adapters have the same MAC address. For example, this problem may occur if you have two network adapters for a virtual machine, and you configure these network adapters to have the same MAC address.

If you open the CIL file in this situation, you see an entry that resembles the following:

> NetworkName="`contoso.com`" Id="e3f3f83c-f050-4d81-9117-xx">
> <MacAddresses>
> <MacAddress>00:11:11:CF:FC:xx</MacAddress>
> <MacAddress>00:11:11:CF:FC:xx</MacAddress>
> </MacAddresses>

Resolution

To resolve this problem, manually delete the duplicate entries from the CIL or to automate this process, use the following source code to create a PowerShell script to

automate.

PowerShell

```
param($inputFilePath, $vamtDirPath)

$cilFilePath = Resolve-Path $inputFilePath;

if (!$cilFilePath)

{

Write-Error "Expected input file name of target CIL";

exit 1;

}

if ($vamtDirPath)

{

$vamtDirPath = Resolve-Path $vamtDirPath;

}

else

{

$prograPath = [environment]::GetEnvironmentVariable("ProgramFiles(x86)");

if (!$prograPath -or $prograPath -eq "")

{

$prograPath = [environment]::GetEnvironmentVariable("ProgramFiles");

}

$vamtDirPath = $prograPath + "\VAMT 2.0"

}

try

{

$assembly = [System.Reflection.Assembly]::LoadFile($vamtDirPath +
"\Vamtrt.dll");

}
```

```
catch

{

Write-Error "Error while attempting to load VAMT assembly. Provide the
correct path to your VAMT installation if VAMT is not installed to the
default directory.";

exit 1;

}

$fileSerializer = new-object
Microsoft.SoftwareLicensing.Vamt.FileSerializer($cilFilePath);

$softwareLicensingData = $fileSerializer.Deserialize();

for ($i = 0; $i -lt $softwareLicensingData.Machines.Length; $i++)

{

$machine = $softwareLicensingData.Machines[$i];

if ($machine.MacAddresses.Count -gt 0)

{

$distinctMacAddrs = new-object
System.Collections.ObjectModel.Collection[string];

foreach ($mac in $machine.MacAddresses)

{

if (!$distinctMacAddrs.Contains($mac))

{

$distinctMacAddrs.Add($mac);

}

}

$machine.MacAddresses.Clear();

foreach ($distinctMac in $distinctMacAddrs)

{

$machine.MacAddresses.Add($distinctMac);

}

}
```

```
}

$fileSerializer.Serialize($softwareLicensingData);
```

Then, follow these steps on a Windows 7 computer:

1. Copy your saved CIL file to c:\script. For example, c:\script\saved.cil
2. Copy the included source code from this KB article into the clipboard
3. Click Start, All Programs, Accessories, Windows PowerShell, "Windows PowerShell ise"
4. In Windows PowerShell, click in the Untitled1.ps1 window
5. Paste in contents of the script from this article
6. Click File, save as, c:\script\ScrubCil.ps1
7. Click Start > All Programs > Accessories > Windows PowerShell, right-click "Windows PowerShell" and choose "Run as Administrator"
8. At the PowerShell prompt type, the following commands

```PowerShell
cd\script
set-executionpolicy unrestricted
.\ScrubCil.ps1 saved.cil
```

How to validate the OEM activation key in Windows 10

Article • 09/23/2021 • 2 minutes to read

This article introduces how to validate the OEM activation key in Windows 10.

Applies to: Windows 10 - all editions
Original KB number: 4346763

Background

Starting at Windows 10 Creators Update (build 1703), Windows activation behavior has changed. The unique OA3 Digital Product Key (DPK) isn't always presented as the currently installed key in the device. Instead, the system behaves as follows:

- Windows 10 (including all versions starting at Windows 10 Creators Update) is deployed to a device by having the appropriate default product key. You can run `slmgr /dli` or `slmgr /dlv` to show the partial default product key instead of the OA3 DPK as the current license in the firmware. The product ID displayed on the **Settings** > **System** > **About** page isn't unique for the Windows 10 key that's being used.

- A device that's running any Windows 10 OEM client edition, such as Windows Home or Windows Professional, and is activated by using the OA3 DPK in the firmware is upgraded to a newer version. For example, it's upgraded from build 1703 to build 1709. However, sometimes running `slmgr /dli` or `slmgr /dlv` doesn't show the OA3 DPK as the current license. Instead, these commands show the default product key.

The behavior is by design. The activation and user experience aren't affected. But OA validation in the factory may be affected as follows:

- The output of the `slmgr /dlv` or `slmgr /dli` command isn't necessarily the last five (5) digits of the injected DPK. So you can no longer rely upon these commands to return the expected results.

Recommendations for validating the product ID against the product key ID of OA3 DPK

Every OEM has a different manufacturing process that has been adopted through years of experience. Specifically, to validate the DPK against the installed Windows 10 edition, we recommend that you don't rely on the output of `slmgr /dlv` or `slmgr/dli`. Instead, use the latest OA3Tool as follows:

- OA3TOOL /Validate

  It runs a validation pass to make sure that:
  - the MSDM table exists.
  - the MSDM table header includes all the required fields.
  - the MSDM table entries exist and comply with the correct formats.

- OA3TOOL /CheckEdition

  Does a cross-check between the injected DPK and the target Windows edition if they match.

Can Microsoft ensure that the system will always activate if I do the recommended steps

The Windows activation system is designed to use the product key that's injected into the firmware of the computer during manufacturing. It automatically activates the device when the device first comes online. This operation is used daily on thousands of devices. As an extra check, OEMs are encouraged to run the complete end-to-end validation process, including activation on a subset of the devices, to validate the user experience with their PCs. If you experience any issues, engage with us through the usual channels.

Why did Microsoft remove the ability to check the last five digits of the product by using slmgr

SLMGR is a legacy tool. Although we haven't updated slmgr, and because of updates in successive system builds, the last five digits of the product key that are shown by `slmgr /dlv` or `/dli` don't match the product key injected into the system BIOS. It's by design. We have no intentions of validating SLMGR for every Windows 10 release or making any other changes. We are very open to feedback regarding the OA3 tool and more capabilities we can add to it to improve the manufacturing flow.

The KMS current count does not increase when you add new Windows Vista or Windows 7-based client computers to the network

Article • 09/23/2021 • 4 minutes to read

This article provides help to fix a problem where the number of clients in a Key Management Server (KMS) computer doesn't increase when you add new Windows Vista-based client computers to the network.

Applies to: Windows 7 Service Pack 1
Original KB number: 929829

Symptoms

When you run the Slmgr.vbs script on a Key Management Server (KMS) computer, you verify that the number of client computers does not increase when you add new Windows-based client computers to the network. Additionally, you may see the following event in the Key Management Service event log for each new Windows-based client computer that you add to the network.

When you run the Slmgr.vbs script together with the `-dli` argument, the client computer count information does not increase as expected. In the following event that is logged in the Key Management Service event log, the current count remains the same.

Cause

This issue can occur when Windows-based client computers that you add to the network have identical KMS client machine IDs (CMIDs). The current count number increases on a KMS computer when the client computers have different CMIDs. Two or more computers can have the same CMIDs in the either of the following scenarios:

- The custom Windows image that you use to install the client computer is generated even though you do not run the System Preparation tool (Sysprep.exe) together with the /generalize option.
- The custom Windows image is generated together with the /generalize option. However, you specify the <SkipRearm> setting in the Unattended.xml file.

To verify that client computers have identical CMIDs, follow these steps:

1. On one of the Windows-based client computers, click **Start**, point to **Programs**, point to **Accessories**, right-click **Command Prompt** and then click **Run as Administrator**. If you are prompted for an administrator password or for a confirmation, type the password, or click **Allow**.
2. At the command prompt, type the following command, and then press ENTER:
   `cscript c:\windows\system32\slmgr.vbs -dli`
3. Examine the following results, and note the CMID.
4. Repeat steps 1 through 4 on a second Windows-based client computer. Verify that the CMID of the second client computer is identical to the CMID of first computer.

Resolution

We recommend that you rebuild the base image that is used to deploy the affected computers as soon as you determine whether they have identical CMIDs.

Workaround

The workaround is valid only if the /generalize option was used in the image that was used to install Windows-based clients. This option is required when you deploy multiple images. To determine whether the /generalize option was used in the image, follow these steps:

1. On one of the affected computers, click **Start**, and then type C:\Windows\System32\sysprep\Panther\setupact.log.
2. Examine the "SYSPRP ParseCommands: Found" lines as shown in the following sample log file:

   > Info [0x0f004e] SYSPRP Initialized SysPrep log at C:\Windows\System32\sysprep\Panther
   >
   > Info [0x0f0054] SYSPRP ValidateUser:User has required privileges to sysprep machine
   > Info [0x0f0056] SYSPRP ValidateVersion:OS version is okay
   > Info [0x0f005c] SYSPRP ScreenSaver:Successfully disabled screen saver for sysprep
   > Info [0x0f007e] SYSPRP FCreateTagFile:Tag file C:\Windows\System32\sysprep\Sysprep_succeeded.tag does not already exist,

> no need to delete anything
> Info [0x0f005f] SYSPRP ParseCommands:Found supported command line option 'UNATTEND'
> Info [0x0f005f] SYSPRP ParseCommands:Found supported command line option 'OOBE'
> Info [0x0f005f] SYSPRP ParseCommands:Found supported command line option 'SHUTDOWN'
> Info [0x0f005f] SYSPRP ParseCommands:Found supported command line option 'GENERALIZE'

3. If the /generalize option is present, confirm that this option was used on the computer that created the base image.

4. If the /generalize option was used and you have computers that have identical CMIDs, follow these steps to rearm the affected computers and rebuild the base image. Make sure that you do not use the <SkipRearm> setting is not used:

   a. On one of the Windows-base client computers, click **Start**, point to **Programs**, point to **Accessories**, right-click **Command Prompt**, and then click **Run as Administrator**.

      If you are prompted for an administrator password or for confirmation, type the password, or click **Allow**.

   b. At the command prompt, type the following command, and then press ENTER:
      `cscript c:\windows\system32\slmgr.vbs -rearm`

   c. Restart the computer.

If the base image was not generated by using Sysprep with the /generalize option, you must rebuild the base image, and then reinstall Windows on the clients. If you use an Unattended.xml file when you rebuild the base image, make sure that the <SkipRearm> setting is not used. For more information about the <SkipRearm> setting, see the Windows Automated Installation Kit (Windows AIK) documentation.

More information

To reset the activation timer and to set a unique CMID, the Rearm process must run on the destination computer. This process is used to reset the activation state. In Windows, the Rearm process can be run by using one of the following two methods:

- Run Sysprep together with the /generalize option on the computer that is used to build the Custom Windows image.
- Force the Rearm process to occur by running the Slmgr.vbs script in an elevated Command Prompt window. For example, type: `cscript c:\windows\system32\slmgr.vbs -rearm`

If the Rearm process did not run because Sysprep was run together with the /generalize option or because you used the <SkipRearm>1</SkipRearm> setting in the Unattended.xml file, client computers may have identical CMIDs. Therefore, the computer count information does not increase as expected. The /generalize option is required when you deploy multiple images. The <SkipRearm> setting should not be used in an unattended file when you deploy computers in a production environment. Therefore, for both cases, we recommend that you rebuild the base image.

"The operation timed out" error when creating a partition using Disk Management console or DiskPart.exe

Article • 04/21/2022 • 2 minutes to read

This article helps to fix the error "The operation timed out" when creating a partition using Disk Management console or DiskPart.exe.

Applies to: Windows Server 2012 R2, Windows Server 2008 R2 Service Pack 1
Original KB number: 2826890

Symptoms

- When you try to create a new volume in Disk Management (diskmgmt.msc), you may receive the following error message:

  > The operation failed to complete because the Disk Management console view is not up-to-date. Refresh the view by using the refresh task. If the problem persists, close the Disk Management console, then restart Disk Management or restart the computer.

- If you try to create a new partition using Diskpart.exe, you may receive an error message that is similar to the following ones:

  > Virtual Disk Service error:
  > The operation timed out.
  >
  > Diskpart has referenced an object which is not up-to-date.
  > Refresh the object by using the RESCAN command.
  > If the problem persists exit DiskPart, then restart DiskPart or restart the computer.

- Additionally, you may see a pop-up window with the following information:

  > Found New Hardware
  > Windows needs to install driver software for your Unknown Device

Cause

These problems occur if the volume.inf is missing from `%Systemroot%\inf` folder.

Resolution

To resolve the problem, do the following steps:

1. Open an elevated Command Prompt. To do it, click Start, click All Programs, click Accessories, right-click Command Prompt, and then click Run as administrator.
2. At the command prompt, type the following command and then press Enter: `sfc /verifyonly`
3. If the above command returns stating problems were found, then type the following command and then press Enter. Let the command operation complete: `sfc /scannow`
4. Open Windows Explorer and then navigate to `%Systemroot%\inf` folder
5. Verify if *volume.inf* file has been replaced. If the file is not replaced, then you need to copy volume.inf from another computer running the same version of Windows, same version of Service Pack, and same CPU architecture.

A description of the driver

Article • 09/23/2021 • 2 minutes to read

This article describes the device driver requirements for x64-based versions of Windows.

Applies to: Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 896333

Summary

x64-based versions of Microsoft Windows Server 2003 and Microsoft Windows XP Professional x64 Edition require 64-bit device drivers for hardware devices and peripherals. The requirement for 64-bit drivers applies to kernel mode components and to user mode components.

More information

Drivers for devices such as printers, cameras, and scanners are typically user mode components and require 64-bit drivers. Additionally, the drivers that are included in Windows Server 2003 Service Pack 1 are not the same for x86-based and for x64-based versions of Windows. Therefore, devices where 32-bit Microsoft Windows Server 2003 drivers are available might not have 64-bit drivers available for x64-based versions of Windows.

Itanium-based 64-bit drivers are not compatible with x64-based versions of Windows because they are compiled specifically for the Itanium operating system. Drivers that are written for Itanium-based computers will not install correctly on x64-based versions of Windows.

To obtain device drivers that are not included on the installation CD for x64-based versions of Windows, use these methods in the following order:

- Method 1 On the Microsoft Windows Update Web site, search for a driver that is certified by the Windows Hardware Quality Labs (WHQL). To search for a WHQL-certified driver, click **Start**, click **Windows Update**, and then follow the instructions on the Windows Update Web site. Alternatively, you can visit the following Microsoft Web site:
  https://update.microsoft.com
- Method 2 Obtain a WHQL-certified driver from the device manufacturer's Web site. For information about how to search for a WHQL-certified driver on the device

manufacturer's Web site, contact your device manufacturer.

- Method 3 Obtain a beta or non-WHQL-certified driver from the device manufacturer.

> **Important**
>
> We do not recommend drivers that are not WHQL-certified. Microsoft cannot guarantee the compatibility of device drivers that are not WHQL-certified.Drivers that are not WHQL-certified are known as unsigned drivers. Drivers that are WHQL-certified are known as signed drivers.

> **Note**
>
> It is the responsibility of the specific hardware or software vendor to make sure that programs and device drivers are compatible with x64-based versions of Windows.

If you experience problems when you try to install a 64-bit driver that is not included with 64-bit versions of Windows, make sure that the driver's .inf file is correctly decorated.

Technical support for Windows x64 editions

Your hardware manufacturer provides technical support and assistance for Microsoft Windows x64 editions. Your hardware manufacturer provides support because a Windows x64 edition was included with your hardware. Your hardware manufacturer might have customized the Windows x64 edition installation with unique components. Unique components might include specific device drivers or might include optional settings to maximize the performance of the hardware. Microsoft will provide reasonable-effort assistance if you need technical help with your Windows x64 edition. However, you might have to contact your manufacturer directly. Your manufacturer is best qualified to support the software that your manufacturer installed on the hardware.

For product information about Microsoft Windows XP Professional x64 Edition, visit the following Microsoft Web site:
https://www.microsoft.com/windowsxp/64bit/default.mspx
For product information about Microsoft Windows Server 2003 x64 editions, visit the following Microsoft Web site:
https://www.microsoft.com/windowsserver2003/64bit/x64/editions.mspx

A high pitched noise is heard when using Bluetooth headphones in Windows 8

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where a high pitched noise is heard when using Bluetooth headphones.

Applies to: Windows 8
Original KB number: 2800101

Symptoms

Consider the following scenario:

- You have Windows 8 installed on a computer with a Bluetooth transceiver.
- You have Bluetooth A2DP headphones or speakers paired to the Bluetooth transceiver on the computer.
- Music or audio is streamed to the headphones or speakers.

In this scenario, you may hear a high pitched noise coming from the Bluetooth A2DP audio output device. This noise is audible even if the volume of the output device is set to 0.

Resolution

This issue is fixed by going to Windows Update and installing the latest important updates for your computer. If Windows Update is unavailable for your computer, a stand-alone cumulative update package for Windows 8 that has fixes to address this issue and others can be found on the Microsoft Download Center and then searching for KB2785094.

More information

Advanced Audio Distribution Profile (A2DP) is a profile that defines how high-quality audio is streamed to a device over a Bluetooth connection.

Bluetooth speakers don't work after update 4505903 is installed in Windows 10, version 1903

Article • 09/23/2021 • 2 minutes to read

This article provides help to solve an issue where Bluetooth speakers don't work after update 4505903 is installed in Windows 10, version 1903.

Applies to: Windows 10, version 1903
Original KB number: 4518538

Symptoms

After you install update 4505903 in Windows 10, version 1903 on a computer that has an internal speaker installed, you experience one of the following issues:

- A Bluetooth speaker can't connect to the computer.
- A Bluetooth speaker can connect to the computer. However, the speaker output sounds noisy (bad quality).
- A Bluetooth speaker can connect to the computer. However, the sound is generated by the internal speaker instead of the Bluetooth device.

Additionally, in Device Manager, you notice an entry under the **Sound, video and game controllers** node for **Microsoft Bluetooth A2dp Source** that shows a yellow bang (exclamation mark) icon.

Resolution

To resolve this issue, install September 10, 2019—KB4515384 (OS Build 18362.356).

Workaround

To work around this issue, use the System File Checker tool (SFC.exe) to repair missing or corrupted system files. To do this, follow these steps:

1. Open the command console by using administrative authority.
2. At the command prompt, type the `sfc /scannow` command, and then press Enter.

> **Note**
>
> It may take several minutes for the command operation to be completed.

3. After the process is finished, restart the computer.

For more information, see Use the System File Checker tool to repair missing or corrupted system files.

Create a user-defined service

Article • 09/23/2021 • 2 minutes to read

This article provides the steps to create a Windows NT user-defined service.

Applies to: Windows 10 - all editions
Original KB number: 137890

> **Important**
>
> This article contains information about editing the registry. Before you edit the registry, make sure you understand how to restore it if a problem occurs. For information on how to do this, view the **Restoring the Registry** or the **Restoring a Registry Key** online Help topics in Registry Editor.

Summary

The Windows NT Resource Kit provides two utilities that allow you to create a Windows NT user-defined service for Windows NT applications and some 16-bit applications, but not for batch files.

Instrsrv.exe installs and removes system services from Windows NT and Srvany.exe allows any Windows NT application to run as a service.

Steps to create a user-defined service

To create a Windows NT user-defined service, follow these steps:

1. At an MS-DOS command prompt(running CMD.EXE), type the following command:

   ```
   Console

   path \INSTSRV.EXE My Service path \SRVANY.EXE
   ```

   where **path** is the drive and directory of the Windows NT Resource Kit (for example, `C:\RESKIT`) and **My Service** is the name of the service you're creating.

   Example: `C:\Program Files\Resource Kit\Instsrv.exe Notepad C:\Program Files\Resource Kit\Srvany.exe`

> ⓘ **Note**
>
> To verify that the service was created correctly, check the registry to verify that the **ImagePath** value under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\service name` is set to point to SRVANY.EXE. If this is not set correctly, the service will stop shortly after it starts and return an Event ID 7000 (The **service name** failed to start).

> ⚠ **Warning**
>
> Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

For information about how to edit the registry, view the following online Help topics in Registry Editor:

- **Changing Keys And Values**
- **Add and Delete Information in the Registry**
- **Edit Registry Data**

> ⓘ **Note**
>
> You should back up the registry before you edit it.

2. Run Registry Editor (Regedt32.exe) and locate the following subkey:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<My Service>`

3. From the **Edit** menu, select **Add Key**. Type the following entries, and select **OK**:

   - Key Name: **Parameters**
   - Class: <leave blank>

4. Select the **Parameters** key.

5. From the **Edit** menu, select **Add Value**. Type the following entries, and select **OK**:

   - Value Name: **Application**
   - Data Type: REG_SZ
   - String: <path>\<application.ext>

where <path>\<application.ext> is the drive and full path to the application executable including the extension (for example, C:\WinNT\Notepad.exe)

6. Close Registry Editor.

By default, a newly created service is configured to run automatically when the system is restarted. To change this setting to **Manual**, run the Services applet from Control Panel. Then change the **Startup** value to **Manual**. A service set to **Manual** can be started in one of several ways:

- From the Services applet in Control Panel
- From an MS-DOS command prompt, type the following command:

  ```
  Console

  NET START <My Service>
  ```

- Use the Sc.exe utility from the Resource Kit. Type the following command from an MS-DOS command prompt:

  ```
  Console

  <path>\Sc.exe start <My Service>
  ```

  where <path> is the drive and directory of the Windows NT Resource Kit (for example, `C:\Reskit`).

For more information on installing and removing a user-defined service, see the Srvany.wri document provided with the Windows NT Resource Kit utilities (for example, `C:\Reskit\Srvany.wri`). This document can also be found on the Windows NT Resource Kit CD in the `Common\Config` directory.

Desktop icons may not be visible after disconnecting HDMI display when Desktop is in Extended mode

Article • 09/23/2021 • 2 minutes to read

This article helps work around an issue where the Desktop icons aren't visible if the HDMI display is disconnected and the computer is rebooted.

Applies to: Windows 8
Original KB number: 2864242

Symptoms

Consider the following scenario:

- You have a computer that is running Windows 8 in a multi-monitor configuration.
- The "Primary Monitory" is connected via HDMI.
- The Desktop is in Extended mode.

In this scenario, the Desktop icons may not be visible if the HDMI display is disconnected and the computer is rebooted.

Workaround

To work around this issue, press the Windows logo key+P and select "Duplicate" then "PC screen only."

Devices are not working before you log on a computer that's running Windows 10

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue in which devices are not working before you log on a computer that's running Windows 10.

Applies to: Windows 10, version 1709
Original KB number: 4057300

Symptoms

Consider the following scenario:

- You have a computer that's running Windows 10, and the computer is joined to an Active Directory domain.
- The computer has BitLocker or device encryption enabled.
- You enable the **Disable new DMA devices when this computer is locked** policy on the computer. The **Disable new DMA devices when this computer is locked** policy locates in the following path:
  Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption

  > ⓘ **Note**
  >
  > To verify that the policy is set, you can also check the following registry key value:
  > **Path**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE`
  > **Value**: DisableExternalDMAUnderLock
  > **Type**: DWORD
  > The issue occurs when the value is set to **1**.

- You restart the computer.

In this scenario, Peripheral Component Interconnect (PCI) devices that have Bus Master Enabled (BME) set to **0** are not enumerated by the Operating System (OS) until a user successfully logs on. This is by design.

Additionally, after a user logs on, certain internal and external device classes may not work. These include but not limited to:

- Wired network adapters
- Wireless network adapters
- Audio devices
- Pointing devices including Touchpads

Cause

This issue may occur in either of the following conditions:

1. The **Disable new DMA devices when this computer is locked** policy requires that the system firmware correctly set the BME bit for all internal devices during startup and disable the BME bit for all externally exposed PCI ports.

   When system firmware incorrectly clears the BME bit for internal devices during startup, those devices are blocked until a successful user logon.

2. Device drivers cannot handle the BME bit locked by the OS until a user logs on.

   The **Disable new DMA devices when this computer is locked** policy is applied intermittently on Windows 10 Version 1703 computers in specific scenarios. Windows 10, version 1709 computers consistently apply that policy, and this causes firmware or driver issues.

More information

You may experience the following issues based on these conditions:

When driver is correct, and firmware is correct

Internal devices work before and after startup. External PCI devices are correctly blocked until a user logs on.

When driver is correct, and firmware is incorrect

Devices are blocked before a logon but work after a logon. Both internal and external devices that have BME set to **0** are blocked before a logon. After a logon, drivers enumerate correctly.

When driver is incorrect, and firmware is correct

External devices might not work after a logon.

When driver is incorrect, and firmware is incorrect

Internal devices initially blocked by firmware either don't properly enumerate or malfunction after a successful user logon.

Resolution

To fix this issue, install April 23, 2018-KB4093105 (OS Build 16299.402).

Workaround

To work around this problem, configure the **Disable new DMA devices when this computer is locked** to **Not Configured** to disable it on affected system models before you update drivers and firmware.

What is a DLL

Article • 04/12/2022 • 13 minutes to read

This article describes what a dynamic link library (DLL) is and the various issues that may occur when you use DLLs. It also describes some advanced issues that you should consider when developing your own DLLs.

Applies to: Windows 10 - all editions
Original KB number: 815065

Summary

In describing what a DLL is, this article describes dynamic linking methods, DLL dependencies, DLL entry points, exporting DLL functions, and DLL troubleshooting tools.

This article finishes with a high-level comparison of DLLs to the Microsoft .NET Framework assemblies.

For the Windows operating systems, much of the functionality of the operating system is provided by DLL. Additionally, when you run a program on one of these Windows operating systems, much of the functionality of the program may be provided by DLLs. For example, some programs may contain many different modules, and each module of the program is contained and distributed in DLLs.

The use of DLLs helps promote modularization of code, code reuse, efficient memory usage, and reduced disk space. So, the operating system and the programs load faster, run faster, and take less disk space on the computer.

When a program uses a DLL, an issue that is called dependency may cause the program not to run. When a program uses a DLL, a dependency is created. If another program overwrites and breaks this dependency, the original program may not successfully run.

With the introduction of the .NET Framework, most dependency problems have been eliminated by using assemblies.

More information

A DLL is a library that contains code and data that can be used by more than one program at the same time. For example, in Windows operating systems, the Comdlg32 DLL performs common dialog box related functions. Each program can use the

functionality that is contained in this DLL to implement an **Open** dialog box. It helps promote code reuse and efficient memory usage.

By using a DLL, a program can be modularized into separate components. For example, an accounting program may be sold by module. Each module can be loaded into the main program at run time if that module is installed. Because the modules are separate, the load time of the program is faster. And a module is only loaded when that functionality is requested.

Additionally, updates are easier to apply to each module without affecting other parts of the program. For example, you may have a payroll program, and the tax rates change each year. When these changes are isolated to a DLL, you can apply an update without needing to build or install the whole program again.

The following list describes some of the files that are implemented as DLLs in Windows operating systems:

- ActiveX Controls (.ocx) files

  An example of an ActiveX control is a calendar control that lets you select a date from a calendar.

- Control Panel (.cpl) files

  An example of a .cpl file is an item that is located in Control Panel. Each item is a specialized DLL.

- Device driver (.drv) files

  An example of a device driver is a printer driver that controls the printing to a printer.

DLL advantages

The following list describes some of the advantages that are provided when a program uses a DLL:

- Uses fewer resources

  When multiple programs use the same library of functions, a DLL can reduce the duplication of code that is loaded on the disk and in physical memory. It can greatly influence the performance of not just the program that is running in the foreground, but also other programs that are running on the Windows operating system.

- Promotes modular architecture

  A DLL helps promote developing modular programs. It helps you develop large programs that require multiple language versions or a program that requires modular architecture. An example of a modular program is an accounting program that has many modules that can be dynamically loaded at run time.

- Eases deployment and installation

  When a function within a DLL needs an update or a fix, the deployment and installation of the DLL does not require the program to be relinked with the DLL. Additionally, if multiple programs use the same DLL, the multiple programs will all benefit from the update or the fix. This issue may more frequently occur when you use a third-party DLL that is regularly updated or fixed.

DLL dependencies

When a program or a DLL uses a DLL function in another DLL, a dependency is created. The program is no longer self-contained, and the program may experience problems if the dependency is broken. For example, the program may not run if one of the following actions occurs:

- A dependent DLL is upgraded to a new version.
- A dependent DLL is fixed.
- A dependent DLL is overwritten with an earlier version.
- A dependent DLL is removed from the computer.

These actions are known as DLL conflicts. If backward compatibility is not enforced, the program may not successfully run.

The following list describes the changes that have been introduced in Windows 2000 and in later Windows operating systems to help minimize dependency issues:

- Windows File Protection

  In Windows File Protection, the operating system prevents system DLLs from being updated or deleted by an unauthorized agent. When a program installation tries to remove or update a DLL that is defined as a system DLL, Windows File Protection will look for a valid digital signature.

- Private DLLs

  Private DLLs let you isolate a program from changes that are made to shared DLLs. Private DLLs use version-specific information or an empty `.local` file to enforce

the version of the DLL that is used by the program. To use private DLLs, locate your DLLs in the program root folder. Then, for new programs, add version-specific information to the DLL. For old programs, use an empty `.local` file. Each method tells the operating system to use the private DLLs that are located in the program root folder.

DLL troubleshooting tools

Several tools are available to help you troubleshoot DLL problems. The following tools are some of these tools.

Dependency Walker

The Dependency Walker tool can recursively scan for all dependent DLLs that are used by a program. When you open a program in Dependency Walker, Dependency Walker does the following checks:

- Dependency Walker checks for missing DLLs.
- Dependency Walker checks for program files or DLLs that are not valid.
- Dependency Walker checks that import functions and export functions match.
- Dependency Walker checks for circular dependency errors.
- Dependency Walker checks for modules that are not valid because the modules are for a different operating system.

By using Dependency Walker, you can document all the DLLs that a program uses. It may help prevent and correct DLL problems that may occur in the future. Dependency Walker is located in the following directory when you install Visual Studio 6.0:

```
drive\Program Files\Microsoft Visual Studio\Common\Tools
```

DLL Universal Problem Solver

The DLL Universal Problem Solver (DUPS) tool is used to audit, compare, document, and display DLL information. The following list describes the utilities that make up the DUPS tool:

- Dlister.exe

  This utility enumerates all the DLLs on the computer and logs the information to a text file or to a database file.

- Dcomp.exe

This utility compares the DLLs that are listed in two text files and produces a third text file that contains the differences.

- Dtxt2DB.exe

  This utility loads the text files that are created by using the Dlister.exe utility and the Dcomp.exe utility into the dllHell database.

- DlgDtxt2DB.exe

  This utility provides a graphical user interface (GUI) version of the Dtxt2DB.exe utility.

DLL Help database

The DLL Help database helps you locate specific versions of DLLs that are installed by Microsoft software products.

DLL development

This section describes the issues and the requirements that you should consider when you develop your own DLLs.

Types of DLLs

When you load a DLL in an application, two methods of linking let you call the exported DLL functions. The two methods of linking are load-time dynamic linking and run-time dynamic linking.

Load-time dynamic linking

In load-time dynamic linking, an application makes explicit calls to exported DLL functions like local functions. To use load-time dynamic linking, provide a header (.h) file and an import library (.lib) file when you compile and link the application. When you do this, the linker will provide the system with the information that is required to load the DLL and resolve the exported DLL function locations at load time.

Run-time dynamic linking

In run-time dynamic linking, an application calls either the `LoadLibrary` function or the `LoadLibraryEx` function to load the DLL at run time. After the DLL is successfully loaded,

you use the `GetProcAddress` function to obtain the address of the exported DLL function that you want to call. When you use run-time dynamic linking, you do not need an import library file.

The following list describes the application criteria for when to use load-time dynamic linking and when to use run-time dynamic linking:

- Startup performance

  If the initial startup performance of the application is important, you should use run-time dynamic linking.

- Ease of use

  In load-time dynamic linking, the exported DLL functions are like local functions. This makes it easy for you to call these functions.

- Application logic

  In run-time dynamic linking, an application can branch to load different modules as required. It is important when you develop multiple-language versions.

The DLL entry point

When you create a DLL, you can optionally specify an entry point function. The entry point function is called when processes or threads attach themselves to the DLL or detached themselves from the DLL. You can use the entry point function to initialize data structures or to destroy data structures as required by the DLL. Additionally, if the application is multithreaded, you can use thread local storage (TLS) to allocate memory that is private to each thread in the entry point function. The following code is an example of the DLL entry point function.

C++

```
BOOL APIENTRY DllMain(
HANDLE hModule,// Handle to DLL module
DWORD ul_reason_for_call,// Reason for calling function
LPVOID lpReserved ) // Reserved
{
    switch ( ul_reason_for_call )
    {
        case DLL_PROCESS_ATTACHED: // A process is loading the DLL.
        break;
        case DLL_THREAD_ATTACHED: // A process is creating a new thread.
        break;
        case DLL_THREAD_DETACH: // A thread exits normally.
        break;
```

```
        case DLL_PROCESS_DETACH: // A process unloads the DLL.
        break;
    }
    return TRUE;
}
```

When the entry point function returns a FALSE value, the application will not start if you are using load-time dynamic linking. If you are using run-time dynamic linking, only the individual DLL will not load.

The entry point function should only perform simple initialization tasks and should not call any other DLL loading or termination functions. For example, in the entry point function, you should not directly or indirectly call the `LoadLibrary` function or the `LoadLibraryEx` function. Additionally, you should not call the `FreeLibrary` function when the process is terminating.

> ⓘ **Note**
>
> In multithreaded applications, make sure that access to the DLL global data is synchronized (thread safe) to avoid possible data corruption. To do this, use TLS to provide unique data for each thread.

Export DLL functions

To export DLL functions, you can either add a function keyword to the exported DLL functions or create a module definition (.def) file that lists the exported DLL functions.

To use a function keyword, you must declare each function that you want to export with the following keyword:
`__declspec(dllexport)`

To use exported DLL functions in the application, you must declare each function that you want to import with the following keyword: `__declspec(dllimport)`

Typically, you would use one header file that has a define statement and an `ifdef` statement to separate the export statement and the `import` statement.

You can also use a module definition file to declare exported DLL functions. When you use a module definition file, you do not have to add the function keyword to the exported DLL functions. In the module definition file, you declare the `LIBRARY` statement and the `EXPORTS` statement for the DLL. The following code is an example of a definition file.

C++

```
// SampleDLL.def
//
LIBRARY "sampleDLL"
EXPORTS HelloWorld
```

Sample DLL and application

In Visual C++ 6.0, you can create a DLL by selecting either the **Win32 Dynamic-Link Library** project type or the **MFC AppWizard (dll)** project type.

The following code is an example of a DLL that was created in Visual C++ by using the **Win32 Dynamic-Link Library** project type.

C++

```
// SampleDLL.cpp
//

#include "stdafx.h"
#define EXPORTING_DLL
#include "sampleDLL.h"
BOOL APIENTRY DllMain( HANDLE hModule, DWORD ul_reason_for_call, LPVOID
lpReserved
)
{
    return TRUE;
}

void HelloWorld()
{
    MessageBox( NULL, TEXT("Hello World"), TEXT("In a DLL"), MB_OK);
}

// File: SampleDLL.h
//
#ifndef INDLL_H
    #define INDLL_H
    #ifdef EXPORTING_DLL
        extern __declspec(dllexport) void HelloWorld();
    #else
        extern __declspec(dllimport) void HelloWorld();
    #endif

#endif
```

The following code is an example of a **Win32 Application** project that calls the exported DLL function in the SampleDLL DLL.

C++

```
// SampleApp.cpp
//
#include "stdafx.h"
#include "sampleDLL.h"
int APIENTRY WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR
lpCmdLine, int nCmdShow)
{
    HelloWorld();
    return 0;
}
```

> **Note**
>
> In load-time dynamic linking, you must link the SampleDLL.lib import library that is created when you build the SampleDLL project.

In run-time dynamic linking, you use code that is similar to the following code to call the SampleDLL.dll exported DLL function.

C++

```
...
typedef VOID (*DLLPROC) (LPTSTR);
...
HINSTANCE hinstDLL;
DLLPROC HelloWorld;
BOOL fFreeDLL;

hinstDLL = LoadLibrary("sampleDLL.dll");
if (hinstDLL != NULL)
{
    HelloWorld = (DLLPROC) GetProcAddress(hinstDLL, "HelloWorld");
    if (HelloWorld != NULL)
        (HelloWorld);
    fFreeDLL = FreeLibrary(hinstDLL);
}
...
```

When you compile and link the SampleDLL application, the Windows operating system searches for the SampleDLL DLL in the following locations in this order:

1. The application folder
2. The current folder
3. The Windows system folder

> ⓘ **Note**
>
> The GetSystemDirectory function returns the path of the Windows system folder.

4. The Windows folder

> ⓘ **Note**
>
> The GetWindowsDirectory function returns the path of the Windows folder.

The .NET Framework assembly

With the introduction of .NET and the .NET Framework, most of the problems that are associated with DLLs have been eliminated by using assemblies. An assembly is a logical unit of functionality that runs under the control of the .NET common language runtime (CLR). An assembly physically exists as a .dll file or as an .exe file. However, internally an assembly is different from a Microsoft Win32 DLL.

An assembly file contains an assembly manifest, type metadata, Microsoft intermediate language (MSIL) code, and other resources. The assembly manifest contains the assembly metadata that provides all the information that is required for an assembly to be self-describing. The following information is included in the assembly manifest:

- Assembly name
- Version information
- Culture information
- Strong name information
- The assembly list of files
- Type reference information
- Referenced and dependent assembly information

The MSIL code that is contained in the assembly cannot be directly executed. Instead, MSIL code execution is managed through the CLR. By default, when you create an assembly, the assembly is private to the application. To create a shared assembly requires that you assign a strong name to the assembly and then publish the assembly in the global assembly cache.

The following list describes some of the features of assemblies compared to the features of Win32 DLLs:

- Self-describing

  When you create an assembly, all the information that is required for the CLR to run the assembly is contained in the assembly manifest. The assembly manifest contains a list of the dependent assemblies. Therefore, the CLR can maintain a consistent set of assemblies that are used in the application. In Win32 DLLs, you cannot maintain consistency between a set of DLLs that are used in an application when you use shared DLLs.

- Versioning

  In an assembly manifest, version information is recorded and enforced by the CLR. Additionally, version policies let you enforce version-specific usage. In Win32 DLLs, versioning can't be enforced by the operating system. You must make sure that DLLs are backward compatible.

- Side-by-side deployment

  Assemblies support side-by-side deployment. One application can use one version of an assembly, and another application can use a different version of an assembly. Starting in Windows 2000, side-by-side deployment is supported by locating DLLs in the application folder. Additionally, Windows File Protection prevents system DLLs from being overwritten or replaced by an unauthorized agent.

- Self-containment and isolation

  An application that is developed by using an assembly can be self-contained and isolated from other applications that are running on the computer. This feature helps you create zero-impact installations.

- Execution

  An assembly is run under the security permissions that are supplied in the assembly manifest and that are controlled by the CLR.

- Language independent

  An assembly can be developed by using any one of the supported .NET languages. For example, you can develop an assembly in Microsoft Visual C#, and then use the assembly in a Visual Basic .NET project.

References

- Deploying and Configuring Applications

- Assemblies
- Run-Time Dynamic Linking
- Thread Local Storage

Error message when you access a USB storage device after resuming from suspend

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an error that occurs when you access a USB storage device after resuming from suspend.

Applies to: Windows 10 - all editions
Original KB number: 323754

Symptoms

If you try to use a Universal Serial Bus (USB) storage device immediately after you resume your computer from suspend, you may receive the following error message:

> **X** :\ drive is not accessible. The request could not be performed because of an I/O device error.

You continue to receive the error message when you try to use the USB storage device until you either remove and reattach the device, or you restart the computer. This problem may occur with any USB storage device such as floppy disk drives, hard disks, or CD-ROM drives.

Cause

This problem occurs with some USB 1.x storage devices that are attached to a USB 2.0 controller in Windows 2000 with the USB 2.0 update installed.

Resolution

To resolve this problem, obtain and install the updated Usbhub.sys file from the hotfix.

Workaround

To work around this problem, wait approximately 10 seconds after you resume your computer before you try to use the USB 1.x storage device.

If you do not use any USB 2.0 devices on the computer, another workaround is to turn off the USB 2.0 controller in Device Manager. After you turn off the USB 2.0 controller, the problem that is described earlier in this article with USB 1.x devices does not occur.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed at the beginning of this article.

More information

After you apply the hotfix that is mentioned earlier in this article, the following behaviors change:

- If you try to use a USB 1.x storage device immediately after you resume your computer, the problem may still occur. However, the problem does not occur if you then try to use the storage device again in a few seconds.
- Soon after you resume your computer, you may receive a **Unsafe Removal of Device** message that mentions the USB 1.x device. You can safely close this box. This message occurs because of a Windows timing issue that involves powering up both the USB companion controller driver stack and the Enhanced Host Controller interface (EHCI) stack after resuming from suspend.

  If the companion controller root hub driver powers up first, the USB 1.x devices that were attached to the root hub ports when the computer entered suspend are no longer attached. Therefore, the driver informs Plug and Play that the device has been removed. This occurs because the devices were routed to the EHCI controller when the Configure Flag was set, but they are not currently attached to the companion controller.

  When the EHCI controller (for USB 2.0) root hub driver then powers up later, the root hub ports are reset and USB 1.x devices are routed back to the companion controllers. The companion controller hub then enumerates the devices again. They are then detected and become functional.

  This does not affect USB 2.0 devices because they always remain attached to the EHCI controller.

Event ID 219 is logged when a device is plugged into a Windows-based system

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where event ID 219 is logged when a device is plugged into a Windows-based system.

Applies to: Windows 10 - all editions, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2
Original KB number: 974720

Symptoms

When a device is plugged into a Windows-based system, the following warning event Kernel-PnP ID 219 is logged together with the event DriverFrameworks-Usermode ID 10114 in the System log:

> (Logged events)
> Warning xxxx/xx/xx xx:xx:xx Kernel-PnP 219 (212)
> The driver \Driver\WudfRd failed to load for the device xxxx.
> Information xxxx/xx/xx xx:xx:xx: DriverFrameworks-UserMode 10114 Start UMDF reflector
> WUDFPf (part of UMDF) did not load yet. After it does, Windows will start the device again.

Cause

When a UMDF device was connected, UMDF driver for that device will be loaded. The Windows Driver Foundation - User-mode Driver Framework service, which is necessary for loading UMDF driver, will be started triggered by loading the driver.

However, for some cases, when the system tries to load the driver, Windows Driver Foundation - User-mode Driver Framework has not started yet. So the two events above are logged.

Resolution

The driver that Windows tries to load will be retried. Unless the events are logged continuously there is no need to do anything, the events are safe to ignore.

You can confirm the driver is loaded successfully in the **System Information**, and you can confirm the devices are running correctly in the **Device Manager**.

Event ID 7000 or 7026 is logged in the System log on a computer that's running Windows

Article • 09/23/2021 • 2 minutes to read

This article describes a problem in which event ID 7000 or event ID 7026 is logged after you start a computer that's running Windows.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 933757

Symptoms

Event ID 7000 or event ID 7026 is logged in the System log on a computer that's running one of the following operating systems:

- Windows 7 Service Pack 1
- Windows Server 2012 R2

This problem may occur if a device isn't connected to the computer but the driver service of the device is enabled.

Workaround

> **Important**
>
> This article contains information about how to modify the registry. Make sure that you back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, see **How to back up and restore the registry in Windows**.

To work around the problem that's described in the example in the Symptoms section, disable the Cdrom or Parport service in the registry to stop the errors from being logged.

To do this, change the value of the following registry subkeys to 3 (Manual) or 4 (Disabled)：

- Registry key 1
  - Path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\cdrom`
  - Name: Start
  - Type: REG_DWORD
  - Data: 3 or 4

- Registry key 2
  - Path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\parport`
  - Name: Start
  - Type: REG_DWORD
  - Data: 3 or 4

> ⓘ **Note**
>
> If the above registry is changed to 4 (Disabled), the related device isn't usable because a driver used in the device isn't loaded. So if the device will be used in the future, the above registry should be set as 3 (Manual).

Error message when you attach a PCI Express expansion chassis to a Windows-based computer: "Code 12" or "Code 31"

Article • 09/23/2021 • 4 minutes to read

This article provides workarounds for errors that occur when you attach a PCI Express expansion chassis to a computer.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 942959

> **Important**
>
> This article contains information about how to modify the registry. Make sure that you back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base: 322756 How to back up and restore the registry in Windows

Symptoms

Consider the following scenario:

- A PCI Express expansion chassis is connected to a computer.
- There are devices connected to the PCI Express expansion chassis.

In this scenario, the devices may not be enumerated correctly, or they may not start correctly. Additionally, you may receive one of the following error messages when you view the device properties in Device Manager:

- Error 1:

  > This device cannot find enough free resources that it can use. (Code 12)

- Error 2:

> The device is not working properly because Windows cannot load the drivers required for this device. (Code 31)

Cause

Cause of error 1

This issue may occur because of the initial state of the PCI Express bridge device in the expansion chassis. By default, when you start or reset PCI Express bridge devices, the initial values of the limit register for the bridge resource window are less than the initial values of the base register for the bridge resource window. This behavior is interpreted as an indication that the bridge resource window is disabled. Additionally, no bridge resource window requirements for the PCI Express bridge device are generated. Therefore, any PCI Express bridge device that requires resources from the bridge resource window will fail enumeration. In this situation, a Code 12 error is generated.

Cause of error 2

This issue may occur if the operating system runs out of Peripheral Component Interconnect (PCI) bus numbers. Typically, the computer BIOS configures a limited bus-number range for PCI Express bridge devices. When an expansion chassis that contains a PCI Express complex switch together with a deep device hierarchy is added to the computer, the operating system runs out of available bus numbers. Therefore, the system cannot start devices in the expansion chassis.

Workaround

Workaround for error 1

⚠ Warning

Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk. To work around this issue, follow these steps:

1. Click **Start**, type **regedit** in the **Start Search** box, and then click **regedit** in the **Programs** list.

   If you are prompted for an administrator password or for confirmation, type the password, or click **Continue**.

2. Locate the following registry subkey, and then click it:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\PnP\Pci`

3. If the HackFlags registry entry is not present, follow these steps:
   a. On the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
   b. Type HackFlags, and then press ENTER.
   c. On the **Edit** menu, click **Modify**.
   d. In the **Value data** box, type 400, click **Hexadecimal** in the **Base** area, and then click **OK**.
   e. Exit Registry Editor.

4. If the HackFlags registry entry is present, follow these steps:
   a. Right-click **HackFlags**, and then click **Modify**.
   b. In the **Value data** box, type 400, click **Hexadecimal** in the **Base** area, and then click **OK**.
   c. Exit Registry Editor.

Workaround for error 2

> ⚠ **Warning**
>
> Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk. To work around this issue, follow these steps:

1. Click **Start**, type **regedit** in the **Start Search** box, and then click **regedit** in the **Programs** list.

   If you are prompted for an administrator password or for confirmation, type the password, or click **Continue**.

2. Locate the following registry subkey, and then click it:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\PnP\Pci`

3. If the HackFlags registry entry is not present, follow these steps:
   a. On the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
   b. Type HackFlags, and then press ENTER.
   c. On the **Edit** menu, click **Modify**.
   d. In the **Value data** box, type 200, click **Hexadecimal** in the **Base** area, and then click **OK**.
   e. Exit Registry Editor.

4. If the HackFlags registry entry is present, follow these steps:
   a. Right-click **HackFlags**, and then click **Modify**.
   b. In the **Value data** box, type 200, click **Hexadecimal** in the **Base** area, and then click **OK**.
   c. Exit Registry Editor.

Enable the workarounds for error 1 and error 2 at the same time

> ⚠ **Warning**
>
> Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

1. Click **Start**, type **regedit** in the **Start Search** box, and then click **regedit** in the **Programs** list.

   If you are prompted for an administrator password or for confirmation, type the password, or click **Continue**.

2. Locate the following registry subkey, and then click it:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\PnP\Pci`

3. If the HackFlags registry entry is not present, follow these steps:
   a. On the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
   b. Type HackFlags, and then press ENTER.
   c. On the **Edit** menu, click **Modify**.
   d. In the **Value data** box, type 600, click **Hexadecimal** in the **Base** area, and then click **OK**.
   e. Exit Registry Editor.

4. If the HackFlags registry entry is present, follow these steps:
   a. Right-click **HackFlags**, and then click **Modify**.
   b. In the **Value data** box, type 600, click **Hexadecimal** in the **Base** area, and then click **OK**.
   c. Exit Registry Editor.

Firmware update failures in Windows 8.1

Article • 03/24/2022 • 8 minutes to read

This article describes how and why firmware updates occasionally fail in a Windows 8.1 environment.

Applies to: Windows 8.1
Original KB number: 2909710

Summary

Computers that are running Windows may use Windows Update to update their firmware. Specifically, these computers use Windows driver packages to install firmware updates. After a firmware driver package has been installed, Windows hands off the firmware updates to UEFI system firmware for installation during your computer's next restart. UEFI system firmware is provided by your computer manufacturer and is separate from Windows. Windows itself doesn't install firmware updates but instead hands off firmware updates to the UEFI system firmware for your computer.

More information

Firmware updates are provided by your computer manufacturer to help improve the stability and performance of your PC. Sometimes firmware updates may not be installed correctly. UEFI system firmware uses a set of return codes to report back to Windows about the success or failure of a firmware installation attempt. These return codes are available in Device Manager and are also reported by Windows Update. In some cases, Windows Update may try to reinstall firmware updates after the initial attempt, depending on the type of failure.

This article describes how to determine whether your PC is using Windows Update and UEFI to install firmware updates. It also describes what each return code means. Finally, it summarizes the Windows Update notifications that you can expect to receive after a failed firmware installation attempt.

How to tell whether your PC installs firmware updates

Windows PCs that use Windows Update to install firmware updates will have "System Firmware Update" entries in the **View your update history for Windows** page of Windows Update.

To view your update history in Windows Update:

1. On the **Start** screen, type *update history*, and then click **View your update history for Windows**.
2. In the search box, enter *Windows Update*, and then select **View update history**. You can also view the error codes that are returned for a failed firmware update by selecting the failed System Firmware Update entry in your update history. The update history page in Windows Update includes a status column, and this indicates which updates failed to install successfully. You can select the entry and open it to see details about the installation, including the installation status and error details.

A computer that uses UEFI to update firmware may also have entries for updatable firmware components in Device Manager. To determine whether your computer uses UEFI to update firmware, follow these steps:

1. From the computer's desktop, open File Manager.
2. In File Manager, right-click **This PC**, and then click **Properties**.
3. Click **Device Manager**.
4. If your computer is using UEFI to manage firmware, there will be a Firmware group under the PC root of Device Manager. Expand the Firmware group to see each updatable firmware component.

   Firmware that wasn't installed successfully will have a "banged out" (!) entry under the Firmware group.
5. You can right-click a failed firmware component and then click **Properties** to see the error codes that were returned. By combining the preceding two checks, you can determine whether your computer is updating firmware through both Windows Update and UEFI.

> **ⓘ Important**
>
> Firmware entries in Device Manager are not guaranteed to be returned from UEFI. In some cases, Windows drivers may install firmware that then is listed under the Firmware group. If you are uncertain about whether your PC is using UEFI, contact your PC manufacturer. You can also view the Hardware IDs details for a particular firmware resource in its properties. UEFI firmware resources are prepended by UEFI\ in the device hardware ID.

Transient vs. non-transient failure codes

Windows separates UEFI firmware update failures into two categories: transient and non-transient.

Transient failures

Transient failures occur because of temporary conditions such as insufficient battery power or lack of system resources. Windows may try to reinstall firmware updates that fail under these circumstances.

For example, your PC may require a certain level of battery power (for example, 25 percent) to install firmware updates. Firmware updates that have failed to install because of low battery power are always retried after the next computer restart. If your PC doesn't have the required battery power available, firmware updates may fail to install. However, Windows will continue to try to install the firmware update at each restart. This battery level check is enforced by both Windows and your computer's UEFI system firmware to make sure that your PC doesn't lose power during a critical firmware update operation.

> **Important**
>
> Windows and UEFI ignore available A/C power and only check the available battery level of your PC. If your battery does not charge beyond the required level, you may not be able to install future firmware updates. If the battery for your PC does not charge, contact your PC manufacturer.

Windows will make a total of three installation attempts after the next three restarts for other transient failures such as a lack of system resources or other reasons that are returned by your UEFI system firmware. If your firmware update fails to install on the third and final restart, Windows won't try to install the firmware update again, and it will be marked as failed in both Device Manager and Windows Update history. The update won't be tried again until your PC manufacturer releases a new update that replaces the failed update.

Non-transient failures

Non-transient firmware update failures are caused by a condition that can't be repaired. Windows doesn't try to reinstall firmware updates that fail because of non-transient conditions.

Installation of the update won't be retried until your PC manufacturer releases a new update the replaces the failed update.

Windows retries firmware updates as follows.

Error condition	Number of retries
Transient	3
Transient: power condition	No limit

Error condition	Number of retries
Non-transient	0

Windows Update power checks

Because your computer may require a certain level of battery power (for example 25 percent) to install firmware updates, Windows Update monitors your battery power level to prevent your computer from needlessly failing a firmware update during an *interactive install*.

During an interactive install, a user manually checks for updates from the Windows Update control panel or the Settings app and then manually starts the update process. An *automatic background install* occurs in the background, staging the new updates that are available for your PC and notifying you that your PC requires a restart. Most of your updates are installed automatically in the background.

Windows Update will verify that your PC has at least 40-percent battery power before it starts firmware updates during an interactive install. During an automatic background install, Windows Update doesn't check for the 40-percent battery power threshold. This behavior occurs because Windows won't try to restart your PC until you have at least 40-percent battery power. Additionally, it will automatically retry installation of failed firmware updates when the battery charges to 40 percent or more.

Windows Update install type	Battery power check
Interactive Install	Battery power level must be at least 40% for all interactive install attempts. If you try to install firmware with < 40% battery, Windows Update prompts you to "Plug your PC into power, let it fully recharge, and try again."
Automatic Background	None. Firmware will always be staged for the next reboot during automatic background installs. Reboot to complete the install will be enforced only when battery power is greater than 40%.

Error codes

The following table lists the LastAttemptStatus error that's reported by UEFI system firmware and the matching NTSTATUS code that's reported by Windows in both Device Manager and Windows Update history. The table also lists the number of times Windows tries to reinstall firmware for each failure code, and the expected Windows Update behavior and update history for each code.

Contact your PC manufacturer for support with failed firmware updates.

ⓘ Important

- If your PC restarts but does not meet the minimum battery power required by UEFI system firmware, the firmware update may fail to install and will fail with one of the power failure codes in the following table. Windows Update may prompt you to reboot your PC after your battery charges to 40% in the case of a firmware update that has failed a battery power check.
- Windows and UEFI ignore available A/C power and check only the available battery power level. If your battery will not charge above the required level, you may be unable to install future firmware updates. If the battery for your PC does not charge, contact your PC manufacturer.
- Transient failures that are not power-related will transition from displaying a "pending reboot" status in Windows Update to "failed" after the third failed installation attempt.
- Non-transient firmware updates or transient firmware updates that have failed all three install attempts will not be retried until they are replaced by a new firmware update from your PC manufacturer.

LastAttemptStatus	**NTSTATUS**	**Code**	**Retries**	**Windows Update after Automatic Install Attempt**	**Status Shown in Windows Update History**
Success	*STATUS_SUCCESS*	*0x00000000*	*N/A*	*None*	*None*
Error: Unsuccessful	STATUS_UNSUCCESSFUL	0xC0000001	3	Windows Update shows "updates available." Later installation attempts through Windows Update or automatic maintenance will retry the firmware installation.	Pending Restart during the first 3 attempts, then "Failed" with the associated failure code.

LastAttemptStatus	NTSTATUS	Code	Retries	Windows Update after Automatic Install Attempt	Status Shown in Windows Update History
Error: Insufficient Resources	STATUS_INSUFFICIENT_RESOURCES	0xC000009A	3		
Error: Incorrect Version	STATUS_REVISION_MISMATCH	0xC0000059	0	Windows Update no longer shows update as available. No other status is provided.	History shows "Failed" and the associated failure code.
Error: Invalid Image Format	STATUS_INVALID_IMAGE_FORMAT	0xC000007B	0		
Error: Unknown Revision	STATUS_UNKNOWN_REVISION	0xC0000058	0		
Error: No Such File	STATUS_NO_SUCH_FILE	0xC000000F	0		
Error: Authentication Error	STATUS_ACCESS_DENIED	0xC0000022	3	Windows Update shows "updates available." Later installation attempts through Windows Update or automatic maintenance will retry the firmware installation.	Pending restart during the first 3 attempts, then "Failed" with the associated failure code.

LastAttemptStatus	NTSTATUS	Code	Retries	Windows Update after Automatic Install Attempt	Status Shown in Windows Update History
Error: Power Event, AC Not Connected	STATUS_POWER_STATE_INVALID	0xC00002D3	No Limit	Windows Update shows "updates available." 15-minute restart timer will also start immediately after battery is recharged to >= 40%.	Pending restart
Error: Power Event, Insufficient Battery	STATUS_INSUFFICIENT_POWER	0xC00002DE	No Limit		

Hide or disable Devices in Devices and Printers

Article • 09/23/2021 • 2 minutes to read

This article describes how to hide or disable **Devices** in **Devices and Printers**.

Applies to: Windows 10 - all editions
Original KB number: 2018577

Symptoms

There is no way in the Windows interface to hide **Devices** within the **Devices and Printers** GUI.

Resolution

You can hide **Devices and Printers** from Control Panel using the supported GPO and then create a folder to view **Printers** only. To do this, use the policy "Hide specified control panel items" to remove the **Devices and Printers** item from the Control Panel window:

1. Edit a GPO.
2. Navigate to **User Configuration\Policies\Administrative Templates\Control Panel**.
3. Double-click **Hide specified control panel items** in the right pane, select **Enable**, click **Show** button, and type *Microsoft.DevicesAndPrinters*.

Once this policy is in place, go to Regedit and create this following Entry:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\`

Create a new key **{2227a280-3aea-1069-a2de-08002b30309d}**

On the right hand Pane **Edit** the **Default** Key and give it the value **Printers**.

This will create a folder on the Desktop as Printers which when opened gives only the Printer listing.

How to use or reference the Usbser.sys driver from universal serial bus (USB) modem .inf files

Article • 09/23/2021 • 2 minutes to read

This article describes how to use or reference the system-supplied Usbser.sys driver file from a third-party modem .inf file.

Applies to: Windows 10 - all editions
Original KB number: 837637

Summary

Universal serial bus (USB) modem .inf files can both use the Usbser.sys driver and directly reference the Usbser.sys driver from the .inf file. However, we don't recommend this.

Instead, we recommend the following:

- Drivers that are distributed with the operating system use the Usbser.sys driver.
- Drivers that are not distributed with the operating system use the Include directive or the Needs directive. The Include directive is described in the More Information section.

More information

To reference the Usbser.sys driver, we recommend that USB modem .inf files reference the Mdmcpq.inf file.

For example, the DDInstall section of an .inf file uses the Include directive and may be similar to the following:

INF

```
[DDInstall.NT]
include=mdmcpq.inf
CopyFiles=FakeModemCopyFileSection

[DDInstall.NT.Services]
include=mdmcpq.inf
AddService=usbser, 0x00000000, LowerFilter_Service_Inst
```

```
[DDInstall.NT.HW]
include=mdmcpq.inf
AddReg=LowerFilterAddReg
```

The following sections appear in the Mdmcpq.inf file:

- FakeModemCopyFileSection
- LowerFilter_Service_Inst
- LowerFilterAddReg

References

For more information, see the "Device Installation" topic in the Microsoft Windows Driver Development Kit documentation.

Limitations of $WinPeDriver$ when used in conjunction with other driver injection methods

Article • 03/24/2022 • 15 minutes to read

This article provides guidance on including drivers into WinPE and the operating system to be installed so that the driver is available in the WinPE portion of installation and also ends up in the completed operating system installation.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2, Windows Server 2008 R2 Service Pack 1
Original KB number: 2686316

Summary

When adding a driver into installation media, don't mix versions. Use the same version of each driver throughout the media.

There are several different methods for including out-of-box drivers into Winpe (boot.wim) and the target installing operating system (install.wim). If the driver versions don't match, the first driver loaded into memory will be used regardless of PNP ranking rules. Other versions may be marked as 'Bad' drivers that will prevent these drivers from being selected by PNP at a later time. This includes any driver loaded into memory during the boot to WinPE (Winpe phase) of installation. Examples could include injecting drivers into boot.wim via DISM.exe or loading a driver using Drvload.exe to manually load the driver.

Purpose

Consider the following scenario: you're creating a custom Windows Pre-installation Environment (WinPE) image for the purposes of installing Windows operating systems that needs an out-of-box storage controller driver before running Setup.exe to manipulate the disks. Additionally, you want to provide "up-to-date" drivers for inclusion via the \$WinPEDriver$ folder feature of Setup, to include later versions of the same driver.

The $WinPEDriver$ feature is intended as a method to provide drivers at installation time. However, it's a feature of Setup.exe, and as such isn't invoked until after Setup.exe launches. Drivers for present devices that are injected manually into the WinPE boot.wim

driverstore using DISM are loaded into memory at boot time. These two mechanisms are separate, and there are some caveats to using them together.

WinPE doesn't have a built-in mechanism to unload drivers that have been loaded into memory, so any drivers for devices that have already been loaded won't be reloaded once setup.exe starts, as there are already drivers for the device loaded. This error will cause Setup to mark the driver in the $WinPEDriver$ folder as a bad driver, even if it's newer than the driver version injected into WinPE and would otherwise outrank it. Setup has no explicit knowledge of drivers that have been loaded into the boot.wim.

This behavior is by design; however this article will identify a method of accommodating this scenario so these drivers can still be included in the deployable operating system.

More information

Given the above scenario, putting WinPE on a bootable USB Flash Device (UFD) hard drive or thumb stick would be most preferable.

In this document, we're going to be highlighting methods for injecting drivers and launching windows. The following chart briefly shows methods and results of including drivers.

WinPE (in-box native or injected)	**(out-box drivers in $WinPEDriver$)**	**Result (Post OS)**
If WinPE contains driver version X1 injected via Dism.exe	contains X2 version of driver with same driver name	X1 will be carried in post OS installation and X2 will be ignored
If WinPE installs driver X2 using Drvload.exe from $WinPEDriver$	contains X2 version of driver with same driver name	X2 will be carried in post OS installation
if WinPE contains driver X1 that isn't boot-critical (in-box native)	contains no driver	Will use in-box native driver X1. No out of box driver will be available for that device post OS installation

Driver Limitations

Keep in mind that there are some drivers that can be included and/or loaded that may not be functional during WinPE portion of installation. This would include, but isn't limited too; video drivers, wireless adapter drivers, and audio drivers. The behavior described in this document isn't specific to BootCritical drivers (drivers need during

boot-up such as controller drivers for access to hard drive) and is in effect for all drivers loaded during installation/deployment.

Walk through of loading drivers from StartNet.cmd

It's but one method for including the same driver into Windows Preinstallation Environment (WinPE) as well as making it available to the installing operating system; other methods are possible using the information further in this document.

1. Set up the technician's machine:
   a. Install OPK/AIK to supported technicians machine.
   b. Copy Windows bits to be modified to local HDD c:\bin.
   c. Locate/download/extract drivers to include into media.

2. Prepare USB device per web page make sure to name device "INSTALL_WIN7". This name is used later and if you change this, you must change the name in the sample script described in step #6 and the example below (web page links are listed at end of document)

3. Create WinPE files for copy to USB device, open Administrative command prompt and run:
   a. `Copype.cmd <arch> <path>`
   b. `Copy <pathto> winpe.wim to \ISO\sources\boot.wim`

4. Mount boot.wim:
   a. `Dism /get-wiminfo /wimfile:\<pathto>\boot.wim`
   b. `Dism /mount-wim /wimfile:<pathto>\boot.wim /index:1 /mountdir: <pathto>\Mount`

5. Open an Administrative Command Prompt and edit \mount\windows\system32\startnet.cmd (using Notepad.exe or similar).

6. The following sample script identifies USB devices and makes drivers available during WinPE using Drvload.exe. Cut and paste the script into the startnet.cmd file that you've open.

   > ⓘ **Note**
   >
   > You may want to copy the script into notepad.exe or some other text editor first to remove formatting.

   Console

```
wpeinit
:ChkVar
:: Locating USB Device
IF NOT DEFINED usbdrv (
ECHO list vol | diskpart | find "INSTALL_WIN7" > pt.txt
FOR /F "tokens=3" %%a IN (pt.txt) DO (
SET usbdrv=%%a^:
)
del pt.txt /f /q
IF EXIST %usbdrv%\InstallOS.bat call InstallOS.bat
```

7. Save StartNet.cmd and close it.

8. Dismount and commit changes to boot.wim using the following command:

```
Console

Dism /unmount-wim /mountdir:<pathto>mount /commit
```

9. Copy all files in the \ISO folder to a USB Flash Device (should be formatted FAT32 and marked as Active).

10. Create a folder on root of USB Flash Device named $WinpeDriver$.

11. Copy drivers into this folder (for example <USB_drv>\$WinpeDriver$\DriverX).

12. Open Administrative cmd prompt and create file <USB_drv>\InstallOS.bat, cutting and pasting the following line into the batch file:
drvload %usbdrv%\$winpedriver$\<device>\filename.INF

13. To include Windows OS installation source files from DVD:
    a. Create the following folder on the USB thumbstick: <USB_drv>\<OS>\Sources (for example e:\Win2008r2x64\Sources).
    b. Select and copy DVD\sources* to <USB_drv>\<OS>\sources (you may exclude boot.wim)
    c. To manually launch setup.exe when booted to WinPE, select <USB_drv>\<OS>\Sources\Setup.exe and add any appropriate switches as needed.
    d. For fully automated deployment, add the following line to the InstallOS.bat file, adding any appropriate switches:
    %usbdrv%\<OS>\Sources\Setup.exe

14. TEST by booting to a USB device on TEST machine

Methods for making drivers available to WinPE

Methods for including drivers into WinPE include:

1. Image build time injection via DISM.exe - Places driver in the Driverstore of the WinPE image and it's selected via Plug and Play at WinPE boot time. It doesn't propagate to the installed OS. For this method you must mount the WIM files for access, inject the driver, and then save and commit the changes to the WIM.

   Steps for gathering information, mounting, injecting, and unmounting WIM:
   a. `DISM /get-wiminfo /wimfile:<pathto>boot.wim`
   b. `DISM /mount-wim /wimfile:<pathto>boot.wim /index:n /mountdir:<pathto>mount`
   c. `DISM /add-driver /image:<pathto>mount / driverpath:<pathto>driverINF` [and conversely `/remove-driver` if needed]
   d. `DISM /unmount-wim /commit /mountdir:<pathto>mount`

2. Runtime driver load via Drvload.exe - Loads driver into memory and starts the device. Doesn't propagate the driver to the installed OS.

3. Runtime driver load via Devcon.exe - Devcon is provided via sample source code in the Windows Device Driver Kit (DDK)/Windows Driver Kit (WDK). You must create and compile your own copy. Devcon is used to manipulate drivers, such as loading drivers into memory and starting devices. Doesn't propagate the driver to the installed OS. (Link in References section)

4. $WinPEDriver$ folder- Setup.exe will attempt to load all drivers in the $WinPEDriver$ directory into memory, and also will schedule them for injection into the installing OS.

5. Runtime answer file (unattend.xml) with DriverPath - Path (and credentials if necessary) must be provided in unattend.xml. It's used to access files in central repository that can be on a network share or local. Setup will attempt to load all drivers in the driver store provided in the unattend.xml and also will schedule them for injection into the installed OS.

Launch Windows installation

There are several methods for launching the installation of the operating system from WinPE, including:

1. Injecting setup packages into boot.wim.
   a. Custom WinPE can be modified to auto launch Windows Setup.exe.
   b. Can also be used for language packs and scripting support.
2. Launching setup.exe from startnet.cmd or winpeshl.ini.
   a. locate USB stick/Hdd

   b. Launch \path\setup.exe </switches>
3. Custom front end to replace cmd.exe (see links for Windows RE in reference section).
4. Booting from regular Windows Setup media, which first boots up to WinPE (Boot.wim) and can take input from attached USB device or network storage. This method isn't discussed in this article.

Methods for adding drivers to Windows

Next, following the progression from installation to inclusion of out-of-box drivers, there are a few methods available to include out-of-box drivers in Windows:

1. Dism.exe
   a. `Dism /get-wiminfo /wimfile:<pathto>Install.wim`
   b. `Dism /mount-wim /wimfile:<pathto>Install.wim /index:n /mountdir:<pathto>mount`
   c. `Dism /add-driver [and conversely /remove-driver] /image:<pathto>mount /driverpath:<pathto>driverINF`
   d. `Dism /unmounts-wim /commit /mountdir:<pathto>mount`
2. \$WinPEDriver$
3. Running a script during unattended installation
   a. unattend.xml (driverstore) in WinPE and Audit Mode (more information is in the References and Links section).
   b. Setupcomplete.cmd can be used for driver injection, but is advised against as it's a poor user experience and can cause delays in booting to the desktop for the first time.
4. Drvload.exe
   a. Only injects drivers into the currently running OS, which if there's WinPE is typically RAM disk.
   b. Drvload <pathto.INF> (can be scripted in startnet.cmd (see examples))

> ⓘ **Note**
>
> If the driver to be used has the same name as an in-box driver (natively included in image) these newly injected drivers will not be used by the booting operating system and you should contact the driver manufacture for updated drivers. (If familiar with the Windows Logo Kit (WLK), see Devfund0005)
>
> If a driver is loaded during WinPE pass (initial boot) there is no native mechanism in place to remove that driver until the operating system reboots.

There are multiple methods for each step of the process of adding drivers to Windows. The methods provide for an extensible and malleable deployment scenario. You'll want to determine which method below works best for the given situation.

Detailed instructions for including out of box drivers in WinPE

Necessary setup/tools:

- Technicians computer - computer used to build/manipulate installation media
- OPK / AIK installed
- USB/UFD or DVD

Using DISM.exe:

1. Install either the OEM Preinstallation Kit (OPK) or the Windows Automated Installation Kit (Windows AIK)
2. Click on **Start** > **Programs** > **Windows OPK** (or **Windows AIK**) and open an Administrative Deployment Tools Command Prompt.
3. Copy boot.wim to the hard drive (ex. c:\Bin). You can also generate new WinPE using Copype.cmd; however, this will not automatically launch setup.exe without additional customizations.
4. Use DISM to identify the number of indexes in the boot.wim. If you're copying the boot.wim from installation media it will have two indexes. Typically we'll modify index #2; otherwise, index #1.
   `dism /get-wiminfo /wimfile:<wim_file>`

   > ⓘ **Note**
   >
   > Files injected into one index will not be available to other indices.
5. Create a 'Mount' folder (ex. c:\Bin\mount)
6. Use DISM to mount the wim.
   `DISM /mount-wim /wimfile:c:\bin\boot.wim /index:1 /mountdir:c:\bin\mount`
7. Place driver in locatable folder (ex. c:\bin\driver).
8. Use DISM to add the driver to the mounted WIM image.
   `dism /image:c:\bin\mount /Add-Driver /driverpath:<path to INF>`
9. Confirm success by checking the DISM log or ensuring that DISM returns completion at the command prompt.
10. Unmount and commit changes to Boot.wim. Close all handles to any open windows that may be open below c:\bin\mount before running this command

(also make sure that the command prompt is at or above the c:\bin directory structure).
`dism /unmount-wim /mountdir:c:\bin\mount /commit`

11. Once DISM successfully unmounts WIM, we can set up things for moving to USB/DVD. If you get an error during dismount, you may want to remount the wim to confirm that the packages were injected. DISM parameters `/cleanup-wim` and `/get-packages` may be helpful here. Refer to the References and Links section at the end of this document for instructions on creating bootable WinPE media on an optical or USB flash drive.

Using \$WinpeDriver$

$WinpeDrivers$ is an additional folder structure that Setup.exe looks for and if found, is parsed to pull in additional drivers. Setup will recursively parse files and folders under this \$WinpeDriver$ folder looking for *.INF files and attempts to install these discovered drivers into the driverstore.

Folder structure can look something like this on the root of the USB device:

\$WinpeDriver$
└\WiFi
└\Wireless1
└Wireless.INF
└Wireless.SYS
└Wireless.CAT (Needed by operating system)

> ⓘ **Note**
>
> If you look in the \Windows\Panther\Setupact.log you can see reference to this folder: *PnPIBS: Checking for pre-configured driver paths ...*
> *PnPIBS: Checking for pre-configured driver directory C:$WinPEDriver$.*
> *PnPIBS: Checking for pre-configured driver directory D:$WinPEDriver$.*
> *PnPIBS: Checking for pre-configured driver directory E:$WinPEDriver$.*
> *PnPIBS: Checking for pre-configured driver directory X:$WinPEDriver$.*

Using Unattended answer file (unattend.xml/autounattend.xml)

Windows can automatically look for an unattended answer file on the root of mounted drives if the files are named autounattend.xml. Windows will also pick up an unattended

answer file if launched with Setup.exe using switches. This answer file can provide information to the installing operating system for such things as drive configuration, product key, computer name, and path to driver store, OEM company information, and many other things. Documentation on how to add a driver to the unattend.xml can be found at the end of this document in the References and Links section.

Below is an example snippet of an AutoUnattend.xml with Drvstore from an AIK Unattend.chm. The XML output specifies the UNC path to additional locations for device drivers and the credentials used to access the network paths.

XML

```
<DriverPaths>
<!-- First PathAndCredentials list item -->
   <PathAndCredentials wcm:action="add" wcm:keyValue="1">
        <Path>\\myFirstDriverPath\DriversFolder</Path>
        <Credentials>
                <Domain>MyDomain</Domain>
                <Username>MyUsername</Username>
                <Password>MyPassword</Password>
        </Credentials>
   </PathAndCredentials>
<!-- Second PathAndCredentials list item -->
   <PathAndCredentials wcm:action="add" wcm:keyValue="2">
      <Path>C:\Drivers</Path>
      <Credentials>
         <Domain>MyComputerName</Domain>
         <Username>MyUsername</Username>
         <Password>MyPassword</Password>
      </Credentials>
   </PathAndCredentials>
</DriverPaths>
```

Using Drvload.exe

Drvload is a tool in WinPE used to add in drivers once you're booted up to the built-in WinPE Command Prompt. When using Drvload, the drivers will need to be identified and placed somewhere. WinPE's startnet.cmd can be used to script Drvload, as well as either of the following actions while booting or booted to WinPE:

1. Running scripts to:
   a. Identify installation media, usually a USB device.
   b. Add out of box drivers
   c. Configure hard drives and recovery partitions
   d. Launch setup.exe or apply WIMs as needed.

2. Post deployment/application of WIM validationFor developers that want to create their own tool to use for injecting or manipulating drivers, DevCon.exe may be a useful utility. For more information on DevCon.exe, see the References and Links section.

Example startnet.cmd

As a means of scripting/automating the installation, the USB device needs to be identified since this is the location of the additional drivers. This example uses a script in WinPE that is autorun on startup to detect the USB drive. This script launches another script to install drivers using Drvload.exe in the WinPE stage of setup. The script is outside of the WIM file so it can easily be modified.

Methods for identifying installation media using WinPE Startnet.cmd (first file launched in default WinPE):

1. First there needs to be a way to automate the identification of the installation media in the WinPE Startnet.cmd, which is the first file launched in a default WinPE configuration. There are one of two ways you can do this:

    - Create a bootable WinPE USB flash drive with a disk volume label of "INSTALL_WIN7". Then put the following lines at the beginning of startnet.cmd to look for the "INSTALL_WIN7" disk volume label:

      Console

      ```
      "INSTALL_WIN7" disk volume label:
      :ChkVar
      :: Locating USB Device
      IF NOT DEFINED usbdrv (
      ECHO list vol | diskpart | find "INSTALL_WIN7" > pt.txt
      FOR /F "tokens=3" %%a IN (pt.txt) DO (
      SET usbdrv=%%a^:
      )
      del pt.txt /f /q
      ```

    - Create 'tag' files on the media as an alternative drive location method for comparison:

      Console

      ```
      :SetOSvar
      @echo off
      IF NOT DEFINED usbdrv (
      ECHO locating OS drive
      FOR %%b IN ( C D E F G H I J K L M N O ) DO (
      ```

```
IF EXIST %%b:\<specialfilename1> IF EXIST %%b:\ <specialfilename2>
(
SET usbdrv=%%b^:
)
)
)
```

> ⓘ **Note**
>
> You will need to ensure that <specialfilename1 & specialfilename2> exist in designated location on USB Flash Device.

2. Include the files into the boot.wim that are being used in the startnet.cmd. This will then put the files to the X: drive where they can be accessed via X:\<file name>. As you add files to the boot.wim, this will increase the WIM memory footprint.

3. Once USB drive letter is known, additional scripts for injection of drivers can be launched. Since it is difficult to modify boot.wim frequently (you must mount/unmount and commit changes each time), it is easier to run scripts outside of startnet.cmd. For example, if we create a script called 'InstallOS.bat' at the root of the USB flash drive, we can easily modify this file to make changes to the bootup/automation process as needed.

   Below is an example of the text needed in the startnet.cmd file that will look for 'InstallOS.bat' and if found, launch it:

   Console

   ```
   IF EXIST %usbdrv%\InstallOS.bat call InstallOS.bat
   Echo %time% %date%
   ```

   > ⓘ **Note**
   >
   > As indicated by its name, InstallOS.bat can do much more than just add drivers to WinPE. However, for the purpose of this document additional scripting detail will not be discussed.

4. At this point %usbdrv% is defined with the drive letter for the USB flash device so drivers present in %usbdrv%\$WinpeDriver$ folder can be injected through scripting in the InstallOS.bat.

For example, in InstallOS.bat add `Drvload.exe %usbdrv%\$winpedriver$\<device>\filename.INF`.

Using this method, the driver that is made available for the operating system is first picked up and used by WinPE.

Windows Recovery Environment (WinRE)

WinRE is typically going to be static on the hard drive, either auto-installed during installation or created/customized by OEMs for recovery scenarios. If the WinRE is used to recover the machine to factory defaults, then there really is no method to dynamically update drivers to the latest version. You will have to create an image using injected drivers into all relevant WIM files such as the WinRE.wim/Boot.wim as well as the image to be applied for the operating system. Ensure that these drivers are all the same versions.

Conclusion

If your requirement is to create a WinPE environment that loads out of box drivers prior to running setup.exe, follow the guidelines described in this document in order to end up with the driver you want in the resulting installed operating system. Writing scripts which leverage Drvload.exe launched by startnet.cmd to load specific drivers located in the $WinPeDriver$ folder on a USB flash drive is the most flexible method available. This method allows you to load a driver during the WinPE phase that carries over into the installed operating system. In addition, it allows for maintaining of a central repository for drivers that will allow for flexibility to update these drivers (so as to maintain the latest drivers in your driver store).

References and Links

- Add Device Drivers during Windows Setup
- What Is Deployment Image Servicing and Management?
- Deployment Image Servicing and Management Command-Line Options
- Drvload Command-Line Options
- DevCon
- Understanding Device Drivers and Deployment

- Driver Paths in Unattend.xml
- Add a Package to a Windows PE Image
- What Is Windows RE?
- How Windows RE Works
- Walkthrough: Create a Bootable Windows PE RAM Disk on CD-ROM
- Walkthrough: Create a Bootable Windows PE RAM Disk on a USB Flash Disk
- How Configuration Passes Work
- Copype.cmd
- Windows Automated Installation Kit (AIK) for Win7/2008r2
- Windows OEM Preinstallation Kit (OPK)

> **Note**
>
> You will need an account to be able to download files from the OEM site.

LoadLibrary function returns STATUS_DLL_NOT_FOUND error on impersonate thread in Windows

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where LoadLibrary function returns STATUS_DLL_NOT_FOUND error on impersonate thread in Windows.

Applies to: Windows Server 2019, Windows Server 2016, Windows 10 - all editions
Original KB number: 4015510

Symptoms

In Windows 10 and Windows Server version 1709 or later versions, if you do not grant dynamic-link library (DLL) access to the process token itself when you use the **LoadLibrary** function to load the DLL, you receive a "STATUS_DLL_NOT_FOUND" error message on impersonate threads.

Cause

> **Note**
>
> This behavior is by design in Windows.

This behavior occurs for the following reasons:

- It's assumed that all Windows-based operating systems have access rights to the DLL that's referred to by the process token.
- Regardless of the condition that's described in the preceding bullet point, this problem is more obvious in Windows 10, Windows Server 2016, Windows Server 2019, and Windows Server, version 1909 than in earlier versions of Windows.

Workaround

To work around this issue, make sure that process tokens have access rights to all the executables that the process loads.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the "Applies to" section.

Loss of functionality for some Intel SMBus Controller devices after you update your system through Windows Update

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue that triggers a loss of functionality for some Intel SMBus Controller devices after you update your system from Windows Update.

Applies to: Windows Server 2012 R2, Windows 10 - all editions, Windows 7 Service Pack 1
Original KB number: 4011290

Symptoms

When you update your computer through Windows Update, some Intel SMBus Controller device drivers are unexpectedly overwritten with Intel Chipset Device software. This causes loss of functionality for some affected Intel SMBus Controller devices. This issue applies to the following Windows operating systems:

- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows Server 2012
- Windows 8.1
- Windows Server 2012 R2

Cause

The existing Intel SMBus Controller device provides the operating system with information about the device and hardware. This enables the operating system to display the correct product name for that piece of hardware in Device Manager.

The Intel Chipset Device software does not install device drivers for the Intel SMBus Controller. This causes a loss of device functionality.

To resolve this issue, use one of the following methods.

Resolution 1: Roll back to the previous Intel SMBus Controller device driver

To do this, follow these steps:

1. Open Device Manager. To do this, click **Start**, click **Control Panel**, and then click **Device Manager**.
2. Select **View**, choose **Devices by Type**, and then expand **System Devices**.
3. Double-click the SMBus device, and then click the **Driver** tab.
4. Click **Roll Back Driver** to restore the SMBus Controller device driver.
5. Restart the system.

Resolution 2: Reinstall the SMBus device driver

To do this, do one of the following:

- For Intel Desktop or Server Boards, download and install Intel Desktop Utilities.
- Contact your computer manufacturer for the SMBus driver appropriate for your system.

Resolution 3 (optional): Install the updated Intel Chipset Device software or the Intel Server Chipset driver from Windows Update

To do this, follow these steps:

1. Open Device Manager. To do this, click **Start**, click **Control Panel**, and then click **Device Manager**.
2. Select **View**, choose **Devices by Type**, and then expand **System Devices**.
3. Double-click the Intel chipset device from the list.
4. Click the **Driver** tab, and then click **Update Driver**.

Resolution 4 (optional): Install the updated Intel Chipset Device software or the Intel Server Chipset driver from the Intel Download Center

To do this, follow these steps:

1. Go to the Intel Download Center.

2. Search for **Intel Chipset Device Software (INF Update Utility)** or **Intel Server Chipset Driver**.
3. Follow the installation instructions.

Third-party contact disclaimer

Microsoft provides third-party contact information to help you find additional information about this topic. This contact information may change without notice. Microsoft does not guarantee the accuracy of third-party contact information.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

My media device isn't available in the Devices charm

Article • 09/23/2021 • 2 minutes to read

This article describes how to determine whether your device is certified for Windows 8, and how to change the default policy to show your non-certified devices in the Devices charm in Windows 8.1.

Applies to: Windows 8.1
Original KB number: 2871501

Summary

The Devices charm experience in Windows for streaming video, audio, and photos is designed to work together with devices that are certified for Windows 8. By default, devices that haven't been certified for Windows 8 aren't shown in the Devices charm for Microsoft Store apps.

More information

To determine whether your device is certified for Windows 8, open the **Devices** page in **PC Settings**. To do it, type **Device Settings** from the Start screen, and then tap or select **Device Settings**. You'll see compatible media devices such as a TV or audio speaker organized as Play devices. If your device isn't certified for Windows 8, **Not Windows certified** will be displayed under the device name. If no Play devices are shown, tap or select **Add a device** to find a compatible device on your home network, or **Change network settings** to turn on finding devices automatically. Otherwise, your device may not be compatible with the Devices charm.

To enable the Devices charm for devices not certified for Windows 8 in Windows 8.1, add the following registry key value:

- Registry subkey: `HKEY_LOCAL_MACHINE\Software\Microsoft\PlayTo`
- Value name: ShowNonCertifiedDevices
- Value type: REG_DWORD
- Value data: 1

> **Important**

Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

To add this registry key value, follow these steps:

1. Start Registry Editor. To do it, type regedit.exe on the Start screen, and then tap or select **regedit.exe**.
2. Locate and then select the following registry subkey: `HKEY_LOCAL_MACHINE\Software\Microsoft`
3. On the **Edit** menu, point to **New**, tap or select **Key**, and then type PlayTo.
4. Select the newly added **PlayTo** key, point to **New** on the **Edit** menu, and then tap or select **DWORD Value**.
5. Type *ShowNonCertifiedDevices* in the **Name** field, and then press Enter.
6. Press and hold or right-click **ShowNonCertifiedDevices**, and then tap or select **Modify**.
7. In the **Value data** box, type *1*.
8. Tap or select **OK**.
9. Exit Registry Editor.

Note

- This feature can also be enabled by following the same steps for `HKEY_CURRENT_USER\Software\Microsoft\PlayTo`. However, we recommend that you add this **ShowNonCertifiedDevices** value under a key that is machine-centric rather than user-centric.
- This feature is for users who would prefer to connect to their non-certified devices even if they won't be guaranteed a great experience.
- Devices not certified for Windows 8 may not be compatible with modern formats used by websites and apps in the Store or playback controls such as volume, skip, or seek.

Msinfo32.exe reports an unexpected value for the Display Adapter RAM when the graphics adapter has 2 GB or more of dedicated video memory

Article • 09/23/2021 • 2 minutes to read

This article discusses an issue where Microsoft System Information (Msinfo32.exe) tool reports incorrect Adapter RAM values under **Components** > **Display**.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2495801

Symptoms

Consider the following scenario:

1. You have a graphics adapter that has 2 GB or more of dedicated (on board) video memory.
2. You run the inbox Windows tool MSInfo32.exe and look at the Adapter RAM value under **Components** > **Display**.

In this scenario, the dedicated video memory on the graphics adapter is reported incorrectly under Adapter RAM. Instead of the expected value showing the memory in gigabytes and bytes, you may instead only see an incorrect value in bytes.

Cause

The value that holds the dedicated video memory size and that MSInfo32.exe uses to populate Adapter RAM is stored in the registry as a signed 32-bit integer. As a result, the value is only capable of storing a positive integer that is under 2 GB in size. If the dedicated video memory on the graphics adapter is 2 GB or greater, MSInfo32.exe will incorrectly report the amount and will also display it as a negative number.

Resolution

Microsoft has confirmed that this is a problem.

More information

The following are some examples of what MSInfo32.exe will report for Adapter RAM under the Display component when the graphics adapter has between 1GB and 3GB of dedicated memory.

Dedicated Video Memory Reported by MSInfo32:

- 1GB 1.00 GB (1,073,741,824 bytes)
- 1.5GB 1.50 GB (1,610,612,736 bytes)
- 2GB (2,147,483,648) bytes
- 2.5GB (1,610,612,736) bytes
- 3GB (1,073,741,824) bytes

MSInfo32 will report the exact same number of bytes for 1GB of dedicated video memory as it does for 3GB. The same holds true for 1.5GB and 2.5GB.

Some non-compliant USB 3.0 devices may not function when connected to USB 3.0 ports in Windows 8

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where some non-compliant USB 3.0 devices don't function when connected to USB 3.0 ports in Windows 8.

Applies to: Windows 8
Original KB number: 2792990

Symptoms

When you connect a USB 3.0 device to a Windows 8 system, the USB device may not be properly recognized and the following Device Status message may be displayed in Device Manager:

> This device cannot start. (Code 10)
>
> The USB device returned an invalid serial number string descriptor.

Cause

This issue is due to an error in the hardware. The serial number contained in the device is invalid per the USB Mass Storage Specification.

Resolution

Connect the USB 3.0 device to a USB 2.0 port on the system or contact the manufacturer of the USB 3.0 device for further assistance. Devices that have a Windows 8 logo are guaranteed to be compliant and compatible with Windows 8. To ensure device compatibility, look for the Windows 8 logo when purchasing a device.

Power Management tab is not visible for some Wireless Network adapters with AOAC platforms in Windows 8

Article • 09/23/2021 • 2 minutes to read

This article discusses a by-design behavior where the Power Management tab is no longer available in the Wireless Network advanced properties in an Always-On/Always-Connected (AOAC) platform.

Applies to: Windows 8
Original KB number: 2889143

Summary

Consider the following scenario:

- You have a system that is an AOAC platform.
- The system is running Windows 8.
- You install the July update rollup 2855336.
- After the update is installed, you open up Device Manager.
- You open the Wireless Network adapter properties.

In this scenario, you notice that the **Power Management** tab is no longer available within the advanced driver properties.

More information

This behavior is by design. For Windows 8, update rollup 2855336 implements this change for Wireless adapter miniports on AOAC platforms.

With AOAC platforms, Windows needs to systematically manage the adapter's power state to achieve Connected Standby. Thus, the **Power Management** tab is not provided for the user to uncheck the **Allow the computer to turn off this device to save power** option. On non-AOAC platforms, the **Power Management** tab is retained.

This update rollup also addresses an issue on both platforms, in which the system might not be able to wake up after the system goes to sleep if the wireless adapter supports OID_RECEIVE_FILTER_SET_FILTER and the checkbox **Allow the computer to turn off this**

device to save power is unchecked. This filter is used when an adapter supports NDIS packet coalescing, SR-IOV, or VMQ.

"Cannot load management console" error when you try to run the TPM Management console

Article • 09/23/2021 • 2 minutes to read

This article provides solutions to fix an error that occurs when you try to run the TPM Management console in Windows 10.

Applies to: Windows 10, version 1809
Original KB number: 4026023

Symptoms

Assume that you disable or clear the Trusted Platform Module (TPM) through the BIOS settings on a Windows 10, version 1703-based, or a Windows 10, version 1809-based device. When you try to run the TPM Management console (TPM.msc), you receive the following error message: Cannot load management console.

Resolution

To fix this issue, use one of the following methods, depending on the situation:

Method 1: TPM is cleared in BIOS

If the TPM is cleared through the BIOS settings, close and then restart the TPM Management console (TPM.msc) again.

Method 2: TPM is disabled in BIOS

If the TPM is disabled through the BIOS settings, you have to re-enable it in BIOS or run the following Windows PowerShell command as an administrator:

PowerShell

```
$tpm = gwmi -n root\cimv2\security\microsofttpm win32_tpm
$tpm.SetPhysicalPresenceRequest(6)
```

Note

After you run the command, you must restart the operating system and accept any BIOS prompts.

Status

Microsoft is researching this problem and will post more information in this article when the information becomes available.

References

For more information, see the following Windows Dev Center article:
SetPhysicalPresenceRequest method of the Win32_Tpm class

In all supported versions of Windows, uninstalling a driver through device manager may not remove associated files or applications with that driver

Article • 09/23/2021 • 2 minutes to read

This article provides help to solve an issue where uninstalling a driver through device manager doesn't remove associated files or applications with that driver.

Applies to: Windows 10 - all editions
Original KB number: 2278714

Symptoms

Consider the following scenario:

- You have a third-party driver installed on a system via the third-party installation.
- The driver installer also installs a third-party application or applications.
- You try to uninstall the driver through the Device Manager.

In this scenario, the driver files, as well as the third-party application are not removed. Each time you reboot the machine, or any other action that forces a re-enumeration of plug and play devices, it will try to install the drivers.

Cause

Microsoft has confirmed that this behavior is by design.

Resolution

If you have installed a third-party driver via a third-party installation, it is recommended that Add and Remove programs is used to uninstall third-party driver packages.

USB device drivers are removed unexpectedly after Windows 10 is updated

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue in which USB device drivers are removed unexpectedly after Windows 10 is updated.

Applies to: Windows 10 - all editions
Original KB number: 4098563

Symptoms

Consider the following scenario:

- You have developed an application that works on Windows 10 Long Term Servicing Branch (LTSB).
- The application relies on custom or third-party universal serial bus (USB) device drivers.
- The application logic expects to find these drivers in the INF cache. Therefore, devices are automatically identified without having to specify the driver on each connection.
- You install some Windows updates.

In this scenario, the drivers are silently removed from the INF cache. Therefore, the application cannot use the drivers as expected.

Additionally, when the scenario occurs, the Process Monitor log shows the following chain:

> 11:55:21.8170826 svchost.exe 868 2424 Process Create C:\Program Files\rempl\remsh.exe SUCCESS PID: 3076,
> Command line: "C:\Program Files\rempl\remsh.exe"
> C:\Windows\system32\svchost.exe -k netsvcs 11:56:47.3634292 remsh.exe 3076 4152 Process Create C:\Windows\system32\rundll32.exe SUCCESS PID: 1248,
> Command line: C:\Windows\system32\rundll32.exe
> C:\Windows\system32\pnpclean.dll,RunDLL_PnpClean /DEVICES /DRIVERS /MAXCLEAN "C:\Program Files\rempl\remsh.exe"
> 11:56:47.3634539 rundll32.exe 1248 4152 Process Start SUCCESS Parent PID: 3076,

> Command line: C:\Windows\system32\rundll32.exe C:\Windows\system32\pnpclean.dll,RunDLL_PnpClean /DEVICES /DRIVERS /MAXCLEAN

> ⓘ **Note**
>
> - The parent svchost.exe process is hosting the task scheduler service.
> - The specific scheduled task that is run in this scenario is located in the following path:
>
>   **Task Scheduler (Local)/Task Scheduler Library/Microsoft/Windows/rempl**

Cause

This issue occurs because Windows receives an update reliability tool during a Windows Update installation of KB 4023057. The tool is designed to clean up the INF driver cache as part of its remediation procedures.

Workaround

The applicability rules for the Windows update reliability tool have been improved. In addition, the latest version of this tool (10.0.14393.10020 or a later version) should not cause the issue.

As a workaround, you can completely block the update reliability tool from running. To do this, run the following commands:

Console

```
takeown /f "C:\Program Files\rempl" /r /d y
icacls "C:\Program Files\rempl" /grant administrators:F /t /q
icacls "C:\Program Files\rempl" /deny system:F /t /q
```

> ⓘ **Note**
>
> The Windows update reliability tool is not published to WSUS servers.

Reference

For more information, see the following articles:

Update to Windows 10 Versions 1507, 1511, 1607, and 1703 for update reliability: March 22, 2018

Overview of Windows as a service

Windows 10 doesn't install specific drivers for USB audio devices on the first connection

Article • 09/23/2021 • 2 minutes to read

This article helps to fix an issue in which Windows 10 doesn't install specific drivers for USB audio devices on the first connection.

Applies to: Windows 10, version 1703
Original KB number: 4021854

Symptom

When you connect a USB audio device to a Windows 10 Version 1703-based computer the first time, the operating system detects the device but loads the standard USB audio 2.0 driver (usbaudio2.sys) instead of the specific device driver.

Cause

This issue occurs because the USB audio 2.0 driver (usbaudio2.sys) isn't classified as a generic driver in Windows 10 Version 1703. Therefore, the system assumes that a compatible, nongeneric driver is installed for the device even though the driver is generic.

This issue also causes Windows 10 Version 1703 to postpone the search for other compatible drivers through Windows Update that typically occurs immediately after you install a new device.

Resolution

To fix this issue, use one of the following methods.

Method 1

To resolve this issue, install update 4022716.

Method 2

If the device-specific driver is distributed through Windows Update, you can manually update the driver by using Device Manager. For more information about how to do this, see update drivers in Windows 10 .

Method 3

If the device is not yet connected, first install the device-specific driver, such as by using the appropriate installer. After the device-specific driver is installed, Windows 10 will select that driver instead of the standard USB audio 2.0 driver when you first connect the device.

> **Note**
>
> See the device manufacturer's user guide for specific instructions about how to install the driver.

Method 4

If the driver isn't distributed through Windows Update, you can manually reinstall the driver. To do this, follow these steps:

1. Install the device-specific driver (see Method 2).
2. Open **Device Manager**.
3. Right-click (or tap and hold) the name of the device, and then select **Uninstall**.
4. Restart the computer.

When it restarts, Windows will try to reinstall the device by using the device-specific driver.

Icons for WSD devices may show up incorrectly as a different class under Devices and Printers

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution to an issue where icons for Web Services for Devices (WSD) devices may show up incorrectly as a different class under Devices and Printers.

Applies to: Windows 7 Service Pack 1
Original KB number: 2403006

Symptoms

A WSD device may show the incorrect icon when viewed in Devices and Printers. For example, a WSD printer may show up with a Server icon and appear under Devices instead of showing a printer icon under Printers and Faxes.

Cause

This issue is caused by an incorrect Device Stage package released by Microsoft and available between June 8 and June 22, 2010.

Resolution

To resolve this problem, clear out the Device Stage Metadata Store and download new packages. To do this, follow these steps:

1. Open an elevated (Administrator) Command Prompt.
2. Type `del /s "%systemdrive%\users\%username%\AppData\Local\Microsoft\Device Metadata\\\*.*"` and press Enter.
3. Type *Y* to the **Are you sure (Y/N)** prompt and press Enter.
4. You may need to type *Y* to confirm several more deletions, depending on the number of Device Stage packages currently on your computer. (all of them will be freshly downloaded by Windows)

These steps will delete the cache contents containing the incorrect package and prompt Windows 7 to redownload the appropriate packages with the correct Device Metadata.

Desktop wakes up unexpectedly from sleep or hibernation

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where desktop wakes up unexpectedly from sleep or hibernation.

Applies to: Windows 8
Original KB number: 2799178

Symptoms

A Windows 8 Desktop computer is automatically waking from sleep or hibernation at a certain time even if there is no "ACPI Wake Alarm" system device found by the operating system.

Cause

For Windows 8 desktops or All-in-one computers, under **Action Center** > **Automatic Maintenance**, the **Allow scheduled maintenance to wake up my computer at the scheduled time** checkbox is automatically enabled. Also, the power policy/Advanced settings/Sleep/Allow wake timers will default to Enabled for AC power.

If the desktop machine does not have an "ACPI Wake Alarm" device (or if it is disabled in the BIOS), Windows 8 still uses the Real Time Clock (RTC) to program wake events, assuming the power policy/Advanced settings/Sleep/Allow wake timers is Enabled for AC power.

Windows 8 automatically configures a "Regular Maintenance" event in TaskScheduler to run at 3:00 AM every day. After initial installation of Window 8, Windows Update is preconfigured to initiate the regular maintenance task and wake event to ensure that it is run.

> ⓘ **Note**

On mobile computers, if there is no "ACPI Wake Alarm" device detected, Windows 8 disables "allow wake timers" on all in-box power plans, and **Allow scheduled maintenance to wake up my computer at the scheduled time** is not enabled.

Resolution

To prevent the Regular Maintenance task from waking the machine at 3:00am, go to **Action Center** > **Automatic Maintenance** and disable the **Allow scheduled maintenance to wake up my computer at the scheduled time** checkbox.

More information

When an application schedules a maintenance trigger (such as Windows Update, if it has downloaded a qualified update to be installed under maintenance), the following actions will take place:

1. From an Administrator command prompt, `Powercfg /waketimers` will indicate that the Regular Maintenance task is scheduled to run at 3:00 AM. For example:

   ```
   Console

   C:\\> powercfg /waketimers
   ```

   Timer set by [PROCESS] \Device\HarddiskVolume1\Windows\System32\services.exe expires at 2:59:29 AM on 12/4/2012 Reason: Windows will execute 'NT TASK\Microsoft\Windows\TaskScheduler\Regular Maintenance' scheduled task that requested waking the computer.

2. Event ID: 808 will be logged in the Application and Services Logs/Microsoft/Windows/TaskScheduler/Maintenance log, to indicate the application, which caused the regular maintenance event to be scheduled. For example:

   > Level: Warning
   > Source: TaskScheduler
   > Event ID: 808
   > Maintenance Task "\Microsoft\Windows\WindowsUpdate\AUScheduledInstall" requests computer wakeup during next regular maintenance run.

Any application can schedule a regular maintenance task to run automatically, as described by the following links.

- Being productive in the background – background tasks
- MaintenanceTrigger Class

The first application to make use of the Regular Maintenance task scheduling feature is Windows Update. The .NET Framework NGEN v4.0 utility has also been observed to cause the regular maintenance event to be scheduled.

Devices connected through a Thunderbolt Dock stop working after the computer resumes from a power state

Article • 06/04/2022 • 2 minutes to read

This article provides a workaround for an issue in which devices that are connected through a Thunderbolt Dock stop working after the computer resumes from a power state.

Applies to: Windows Client
Original KB number: 4532436

Symptoms

Consider the following scenario:

- On a computer that's running any version of Windows 10 or Windows 11, you enable Fast Startup.
- On a Thunderbolt Dock, several devices are attached. For example, a keyboard, mouse, and USB encryption key are attached.
- You repeatedly do the following steps:
  - You connect the Thunderbolt Dock to the computer so that devices on the Thunderbolt Dock are enumerated.
  - The system enters or resumes from a Modern Standby, Hibernate (S4), or Soft Off (S5) power state. During this activity, you plug or unplug the dock.

In this scenario, the devices stop working. Device Manager might show yellow exclamation points and **Code 10**, **Code 24**, or **Code 43** for those devices.

Workaround

When the issue occurs, the functionality of the devices can be restored by reattaching the Thunderbolt Dock. If this doesn't work, restart the computer.

References

For more information about Windows power states, see System Power States.

Fast startup causes hibernation or shutdown to fail in Windows 10 or Windows 8.1

Article • 09/23/2021 • 2 minutes to read

This article provides help to solve an issue where the process fails when you try to shut down or hibernate the system on a computer.

Applies to: Windows 10 - all editions
Original KB number: 3211190

Symptoms

When you try to shut down or hibernate the system on a computer that's running Windows 10 or Windows 8.1, the process fails and reverts to the Windows Lock screen.

Additionally, when you go to the **Details** tab in this event and then select friendly view, you may notice the following:

> Binary data:
>
> In Words
>
> 0000: 00000000 00000001 00000000 C004002D
> 0010: 00002005 C0000034 00000000 00000000
> 0020: 00000000 00000000
>
> C0000034 - means STATUS_OBJECT_NAME_NOT_FOUND
>
> C004002D - means IO_DUMP_DRIVER_LOAD_FAILURE

Cause

This issue may occur if Fast Startup is enabled under **Control Panel\All Control Panel Items\Power Options\System Settings**. When Fast Startup is enabled and a user shuts down the computer, all sessions are logged off, and the computer enters hibernation. As part of the hibernation process, Windows initializes the system's memory dump configuration. If the driver is not loaded, it fails to hibernate, and the event that's mentioned in the Symptoms section is logged. This brings you back to the Windows Lock screen.

Resolution

> **ⓘ Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

To resolve this issue, check whether event ID 45 is logged in the System log. If you see this event, verify the contents under the DumpFilters registry value:

1. Open the **Run** box. To do this, press the Windows logo key + R.
2. Type *regedit*, and then press Enter.
3. Locate and click the following registry entry:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\CrashControl\`
4. From the pane on the right, verify the contents under the DumpFilters registry value.
5. Remove everything and make sure that dumpfve.sys is the only value listed.
6. Exit Registry editor.
7. Restart the computer to enable Fast Startup.

Workaround

If you want to shut down the computer without using the Hybrid Shutdown behavior, you can use Shutdown.exe instead. Full shutdown is the default when you use Shutdown.exe, as follows:

```
Console

Shutdown /s /t 0
```

The Shutdown.exe command also includes an optional `/hybrid` parameter that can be used if you want to use the new method:

Console

```
Shutdown /s /hybrid /t 0
```

> **Note**
>
> - The Fast Startup setting doesn't apply to Restart.
> - Fast Startup is enabled by default in Windows.
> - Disabling Fast Startup is not recommended.

More information

During Fast Startup, the kernel session is not closed, but it is hibernated. Fast Startup is a setting that helps the computer start faster after shutdown. Windows does this by saving the kernel session and device drivers (system information) to the hibernate (hiberfil.sys) file on disk instead of closing it when you shut down the computer.

When you restart the computer, this typically means that you want a completely new Windows state, either because you have installed a driver or replaced Windows elements that cannot be replaced without a full restart.

Therefore, the restart process in Windows continues to perform a full boot cycle, without the hibernation performance improvement that's described in this article.

Hard disk usage reaches 100 percent after the computer resumes from Sleep mode

Article • 09/23/2021 • 2 minutes to read

After a Windows 8.1-based computer resumes from Sleep mode, the computer stops responding, and the hard disk usage reaches 100 percent. This article provides a solution to this issue.

Applies to: Windows 8.1
Original KB number: 2922899

Symptoms

After you resume a Windows 8.1-based computer from Sleep mode, the disk usage reaches 100 percent, and then the computer stops responding. This issue occurs when the following conditions are true:

- Device Initiated Power Management (DIPM) is enabled on the computer. Generally, this feature is enabled by changing the power scheme from **Balanced** to **Power Saver**, and by using the powercfg command.
- The computer uses a non-Connected Standby Intel Haswell system that uses a Lynx Point Rev4 chipset.
- The computer uses a SATA drive that doesn't implement Automatic Partial to Slumber (APS) transitions, or there is a problem with implementing it.

Workaround

To work around this issue, follow these steps:

1. Change power plan to **Balanced**.

2. Start Command Prompt as administrator, and then run the following commands:

```
Console

powercfg /setacvalueindex scheme_max sub_disk 0b2d69d7-a2a1-449c-9680-
f91c70521c60 1
powercfg /setdcvalueindex scheme_max sub_disk 0b2d69d7-a2a1-449c-9680-
f91c70521c60 1
```

3. Change the power plan back to **Power Saver**. You can also contact the computer vendor for a BIOS update that may fix the issue.

How to disable and re-enable hibernation on a computer that is running Windows

Article • 09/23/2021 • 2 minutes to read

This article describes how to disable and then re-enable hibernation on a computer that is running Windows.

Applies to: Windows Server 2019, Windows 10 - all editions, Windows Server 2016, Windows 7 Service Pack 1, Windows Server 2012 R2, Windows Server 2008 R2 Service Pack 1
Original KB number: 920730

> ⚠ **Warning**
>
> You may lose data if you make hibernation unavailable and a power loss occurs while the hybrid sleep setting is turned on. When you make hibernation unavailable, hybrid sleep does not work.

How to make hibernation unavailable

1. Press the Windows button on the keyboard to open Start menu or Start screen.
2. Search for **cmd**. In the search results list, right-click **Command Prompt**, and then select **Run as Administrator**.
3. When you are prompted by User Account Control, select **Continue**.
4. At the command prompt, type `powercfg.exe /hibernate off`, and then press Enter.
5. Type *exit*, and then press Enter to close the **Command Prompt** window.

How to make hibernation available

1. Press the Windows button on the keyboard to open Start menu or Start screen.
2. Search for **cmd**. In the search results list, right-click **Command Prompt**, and then select **Run as Administrator**.
3. When you are prompted by User Account Control, select **Continue**.
4. At the command prompt, type `powercfg.exe /hibernate on`, and then press Enter.
5. Type *exit*, and then press Enter to close the Command Prompt window.

More information

The Hiberfil.sys hidden system file is located in the root folder of the drive where the operating system is installed. The Windows Kernel Power Manager reserves this file when you install Windows. The size of this file is approximately equal to how much random access memory (RAM) is installed on the computer.

The computer uses the Hiberfil.sys file to store a copy of the system memory on the hard disk when the hybrid sleep setting is turned on. If this file is not present, the computer cannot hibernate.

Reference

To add the Hibernate option to Start menu, see the Hibernate section of Shut down, sleep, or hibernate your PC.

Wake on LAN (WOL) behavior in Windows 10

Article • 09/23/2021 • 2 minutes to read

This article provides information on how to enable Wake on LAN behavior in different versions of Windows.

Applies to: Windows 10, version 1903, Windows 10, version 1809, Windows 7 Service Pack 1
Original KB number: 2776718

Summary

The Wake on LAN (WOL) feature wakes a computer from a low-power state when a network adapter detects a WOL event. Typically, such an event is a specially constructed Ethernet packet. The default behavior in response to WOL events has changed from Windows 7 to Windows 10.

Windows 7

In Windows 7, the default shutdown operation puts the system into the classic shutdown state (S5). And all devices are put into the lowest power state (D3). WOL from S5 isn't officially supported in Windows 7. However, some network adapters can be left armed for waking if enough residual power is available. So waking from S5 is possible on some systems if enough residual power is supplied to the network adapter, even though the system is in the S5 state and devices are in D3.

Windows 10

In Windows 10, the default shutdown behavior puts the system into the hybrid shutdown (also known as Fast Startup) state (S4). And all devices are put into D3. In this scenario, WOL from S4 or S5 is unsupported. Network adapters are explicitly not armed for WOL in these cases, because users expect zero power consumption and battery drain in the shutdown state. This behavior removes the possibility of invalid wake-ups when an explicit shutdown is requested. So WOL is supported only from sleep (S3), or when the user explicitly requests to enter hibernate (S4) state in Windows 10. Although the target system power state is the same between hybrid shutdown and hibernates (S4), Windows will only explicitly disable WOL when it's a hybrid shutdown transition, and not during a hibernate transition.

> **Note**
>
> the firmware and hardware on some systems may support arming Network Interface Cards (NIC) for wake from S4 or S5, even though Windows isn't involved in the process.

More information

In Windows 10, hybrid shutdown (also known as Fast Startup) (S4) stops user sessions but lets the contents of kernel sessions be written to the hard disk. It enables faster startups.

To disable the S4 state in Windows 10, follow these steps.

> **Note**
>
> We don't recommend that you disable the hybrid shutdown (S4) state.

1. In **Control Panel**, open the **Power Options** item.
2. Select the **Choose what the power buttons do** link.
3. Clear the **Turn on fast startup (recommended)** check box.
4. Select **Save Settings**.

References

For more information, see:

- System Power Actions
- System Power States

Power/shutdown button may be missing from the Windows 8.1 start screen

Article • 03/24/2022 • 2 minutes to read

This article describes an issue where the power/shutdown button is missing from the start screen after you install or upgrade to Windows 8.1.

Applies to: Windows 8.1
Original KB number: 2959188

Summary

After you install or upgrade to Windows 8.1, the power/shutdown button may not be present on the start screen, depending on the kind of hardware that you have.

More information

The following table summarizes when the power/shutdown button should be present on the start screen after you install the Windows 8.1 update:

Device type	Supports Connected Standby	Screen size	Show power/shutdown button by default	Default behavior is customizable by the manufacturer
Slate	Yes	<8.5"	No	No
Slate	No	<8.5"	No	Yes
Slate	Yes	>=8.5"	No	Yes
Slate	No	>=8.5"	Yes	Yes
All other devices	Doesn't matter	All sizes	Yes	Yes

> **Note**
>
> An entry of Slate in the **Device type** column means that the hardware reported a Power_Platform_Role of **PlatformRoleSlate**. To determine what a system is

reporting, run the `powercfg /energy` command, and then notice what is listed for **Platform Role** in the output.

Example of Microsoft Surface behavior for new installations is as follows:

- Surface RT or Surface 2: No power button on start screen
- Surface 3: No power button on start screen
- Surface Pro or Surface Pro 2: Power button on start screen
- Surface Pro 3: No power button on start screen

> **Note**
>
> The images that ship with the Surface 3 and Surface Pro 3 are configured to show the power button. This is a customization that is included with the image.

To change the default behavior when Windows images are being deployed, IT professionals should set the Microsoft-Windows-Shell-Setup ShowPowerButtonOnStartScreen setting for new installations.

The Allow the computer to turn off this device to save power option doesn't remain selected after you restart Windows Vista

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue that the **Allow the computer to turn off this device to save power** option doesn't remain selected after you restart the computer.

Applies to: Windows Vista
Original KB number: 930312

Symptoms

In Windows Vista, you click to select the **Allow the computer to turn off this device to save power** check box. However, when you restart the computer, this check box is cleared.

> ⓘ **Note**
>
> This check box appears on the **Power Management** tab of a **USB Root Hub Properties** dialog box. For more information about how to find this check box, see the **More information** section.

Workaround

To work around this problem, enable the **USB selective suspend** option. To do it, follow these steps:

1. Select **Start**, type power options in the **Start Search** box, and then select **Power Options** in the **Programs** list.

   If you're prompted for an administrator password or confirmation, type your password or select **Continue**.

2. Under the selected power plan, select **Change plan settings**.

3. Select **Change advanced power settings**.

4. In the **Power Options** dialog box, expand **USB settings**, and then expand **USB selective suspend setting**.
5. If you want to enable Windows Vista to turn off the USB root hub when the computer is running on battery power, select **Enabled** in the **On battery** list.
6. If you want to enable Windows Vista to turn off the USB root hub when the computer is plugged in to a power outlet, select **Enabled** in the **Plugged in** list, and then select **OK**.

Status

Microsoft has confirmed that it's a problem in the Microsoft products that are listed in the Applies to section.

More information

To view the **Allow the computer to turn off this device to save power** check box, follow these steps:

1. Select **Start**, type device manager in the **Start Search** box, and then select **Device Manager** in the **Programs** list.

   If you're prompted for an administrator password or confirmation, type your password or select **Continue**.
2. In the **Device Manager** dialog box, expand **Universal Serial Bus controllers**, right-click **USB Root Hub**, and then select **Properties**.
3. In the **USB Root Hub Properties** dialog box, select the **Power Management** tab. The **Allow the computer to turn off this device to save power** check box is displayed.

Updates may not be installed with Fast Startup in Windows 10

Article • 09/23/2021 • 2 minutes to read

This article discusses an issue where Windows updates might not be installed with the Fast Startup feature in Windows 10 after you shut down your computer.

Applies to: Windows 10 - all editions
Original KB number: 4011287

Summary

Windows updates might not be installed on your system after you shut down your computer. This behavior occurs when the Fast Startup feature is enabled. This behavior doesn't occur when you restart your computer.

More information

The Fast Startup feature in Windows 10 allows your computer start up faster after a shutdown. When you shut down your computer, Fast Startup will put your computer into a hibernation state instead of a full shutdown. Fast Startup is enabled by default if your computer is capable of hibernation.

Installation of some Windows updates can be completed only when starting your computer after a full shutdown. Since Fast Startup uses hibernation instead of a full shutdown, installation of those updates will not be completed before a full shutdown. In order to make sure pending updates are completed, you have to choose **Restart** from the **Power** menu.

In environments managed with Microsoft Endpoint Manager Configuration Manager (MEMCM), Fast Startup may delay the completion of updates as well. This has been addressed in MEMCM 2002 and Windows 10 21H1.

Windows Update - additional resources

Article • 09/02/2022 • 3 minutes to read

Applies to: Windows Server 2019, Windows Server 2016, Windows 11, Windows 10

> **Note**
>
> Windows Server 2016 supports policies available in Windows 10, version 1607.
> Windows Server 2019 supports policies available in Windows 10, version 1809.

The following resources provide additional information about using Windows Update.

WSUS troubleshooting

- Troubleshooting issues with WSUS client agents
- How to troubleshoot WSUS
- Error 80244007 when WSUS client scans for updates
- Updates may not be installed with Fast Startup in Windows 10

How do I reset Windows Update components?

- Try using the Windows Update Troubleshooter, which will analyze the situation and reset any components that need it.
- Try the steps in Troubleshoot problems updating Windows 10.
- Try the steps in Fix Windows Update errors.

If all else fails, try resetting the Windows Update Agent by running these commands from an elevated command prompt:

Console

```
net stop wuauserv
rd /s /q %systemroot%\SoftwareDistribution
net start wuauserv
```

Reset Windows Update components manually

1. Open a Windows command prompt. To open a command prompt, select **Start** > **Run**. Copy and paste (or type) *cmd* and then press Enter.

2. Stop the BITS service, the Windows Update service and the Cryptographic service. Type the following commands at a command prompt. Press Enter after you type each command.

```
Console

net stop bits
net stop wuauserv
net stop cryptsvc
```

3. Delete the *qmgr*.dat* files. Type the following command at a command prompt, and then press Enter:

```
Console

Del "%ALLUSERSPROFILE%\Application
Data\Microsoft\Network\Downloader\qmgr*.dat"
```

4. If it is your first attempt at resolving your Windows Update issues by using the steps in this article, go to step 5 without carrying out the steps in step 4. The steps in step 4 should only be performed at this point in the troubleshooting if you can't resolve your Windows Update issues after following all steps but step 4. The steps in step 4 are also performed by the "Aggressive" mode of the Fix it Solution above.

   a. Rename the following folders to `*.BAK`:

   - *%Systemroot%\SoftwareDistribution\DataStore*
   - *%Systemroot%\SoftwareDistribution\Download*
   - *%Systemroot%\System32\catroot2*

   To do this, type the following commands at a command prompt. Press Enter after you type each command.

```
Console

Ren %Systemroot%\SoftwareDistribution\DataStore DataStore.bak
Ren %Systemroot%\SoftwareDistribution\Download Download.bak
Ren %Systemroot%\System32\catroot2 catroot2.bak
```

> **Important**
>
> The reset step below using *sc.exe* will overwrite your existing security ACLs on the BITS and Windows Update service and set them to default. Skip this

step unless the other steps to reset Windows Update components have not resolved the issue.

b. Reset the BITS service and the Windows Update service to the default security descriptor. To do this, type the following commands at a command prompt. Press Enter after you type each command.

```
Console

sc.exe sdset bits D:(A;CI;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)
(A;;CCLCSWLOCRRC;;;SU)
sc.exe sdset wuauserv D:(A;;CCLCSWRPLORC;;;AU)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)
```

5. Type the following command at a command prompt, and then press Enter:

```
Console

cd /d %windir%\system32
```

6. Reregister the BITS files and the Windows Update files. To do this, type the following commands at a command prompt. Press Enter after you type each command.

```
Console

regsvr32.exe atl.dll
regsvr32.exe urlmon.dll
regsvr32.exe mshtml.dll
regsvr32.exe shdocvw.dll
regsvr32.exe browseui.dll
regsvr32.exe jscript.dll
regsvr32.exe vbscript.dll
regsvr32.exe scrrun.dll
regsvr32.exe msxml.dll
regsvr32.exe msxml3.dll
regsvr32.exe msxml6.dll
regsvr32.exe actxprxy.dll
regsvr32.exe softpub.dll
regsvr32.exe wintrust.dll
regsvr32.exe dssenh.dll
regsvr32.exe rsaenh.dll
regsvr32.exe gpkcsp.dll
regsvr32.exe sccbase.dll
regsvr32.exe slbcsp.dll
regsvr32.exe cryptdlg.dll
```

```
regsvr32.exe oleaut32.dll
regsvr32.exe ole32.dll
regsvr32.exe shell32.dll
regsvr32.exe initpki.dll
regsvr32.exe wuapi.dll
regsvr32.exe wuaueng.dll
regsvr32.exe wuaueng1.dll
regsvr32.exe wucltui.dll
regsvr32.exe wups.dll
regsvr32.exe wups2.dll
regsvr32.exe wuweb.dll
regsvr32.exe qmgr.dll
regsvr32.exe qmgrprxy.dll
regsvr32.exe wucltux.dll
regsvr32.exe muweb.dll
regsvr32.exe wuwebv.dll
```

7. Reset Winsock. Type the following command at a command prompt, and then press Enter:

```
Console

netsh winsock reset
```

8. If you're running Windows XP or Windows Server 2003, you have to set the proxy settings. Type the following command at a command prompt, and then press Enter:

```
Console

proxycfg.exe -d
```

9. Restart the BITS service, the Windows Update service and the Cryptographic service. Type the following commands at a command prompt. Press Enter after you type each command.

```
Console

net start bits
net start wuauserv
net start cryptsvc
```

10. If you're running Windows Vista or Windows Server 2008, clear the BITS queue. Type the following command at a command prompt, and then press Enter:

```
Console
```

```
bitsadmin.exe /reset /allusers
```

Windows Update troubleshooting guidance

Article • 08/22/2022 • 5 minutes to read

Try our Virtual Agent - It can help you quickly identify and fix common Windows Update issues

These solutions designed to get you started on Windows Update troubleshooting scenarios.

Troubleshooting checklist

Step 1: Run the diagnostic tool for your version of Windows

- **Windows 7, Windows 2008 R2 or Windows 2008 SP2:** Run the System Readiness (CheckSUR) tool. For more information, see Fix errors that are found in the CheckSUR log file.
- **Windows 8 and later version of Windows:** Open an administrative command prompt window, and then run the following command:

```
cmd
```

```
Dism /online /cleanup-image /restorehealth
```

Step 2: Restart the computer

If the computer didn't restart after a previous update, pending actions may still have to be completed before you can apply new updates.

Step 3: Install the latest servicing stack update

For more information, see Latest Servicing Stack Updates.

Step 4: Check for and fix any Windows file corruption

For more information, see Fix Windows file corruption.

Step 5: Download the update package and try to install the update manually

To do this, follow these steps:

1. Open Microsoft Update Catalog.
2. In the search box, type the update number that you want to download, and then select **Search**.
3. Find the update that applies to your operating system in the search results. Next to that update, select **Add** to add the update to your basket.
4. Select **View basket**, and then select **Download**.
5. To choose a destination for the update, select **Browse**, and then select **Continue**.
6. When the download process finishes, select **Close**.
7. Browse to the download location, and then double-click the download package to install the update.

Common issues and solutions

Error: The update is not applicable to your computer

This error has several possible causes. The following instructions help you identify the specific cause that affects you.

Step 1: Has the update been superseded?

Make sure that the update package contains newer versions of the binaries than the system that you're updating. Alternatively, check that the package is superseded by another new package.

As updates for a component are released, the updated component will supersede an older component that is already on the system. When this occurs, the previous update is marked as superseded. If the update that you're trying to install already has a newer version of the payload on your system, you might receive this error message.

Step 2: Has the update already been installed?

Verify that the package that you're trying to install isn't already installed.

Step 3: Is the update appropriate for this architecture?

1. Verify that the package that you're trying to install matches the Windows version that you're using.

   The Windows version information can be found in the "Applies To" section of the article for each update. For example, Windows Server 2012-only updates can't be installed on Windows Server 2012 R2-based computers.

2. Verify that the package you want to install matches the processor architecture of the Windows version that you're using.

   For example, an x86-based update can't be installed on x64-based installations of Windows.

Step 4: Have all prerequisite updates been installed?

Read the package's related article to find out if the prerequisite updates are installed. For example, if you receive the error message in Windows 8.1 or Windows Server 2012 R2, you might have to install the April 2014 update 2919355 as a prerequisite and one or more prerequisite servicing updates (KB 2919442 and KB 3173424).

To determine whether these prerequisite updates are installed, open a Windows PowerShell window and run the following command:

```
PowerShell

Get-HotFix KB3173424, KB2919355, KB2919442
```

If the updates are installed, the command returns the installed date in the **InstalledOn** section of the output.

The device isn't receiving an update that you deployed

Follow these steps to troubleshoot this issue.

1. Check that the device's updates for the relevant category aren't paused.

   For more information, see Pause feature updates and Pause quality updates.

2. **Feature updates only:** Check to see if the device might have a safeguard hold applied for the given feature update version.

   For more information about safeguard holds, see Safeguard holds and Opt out of safeguard holds.

3. Check that the deployment to which the device is assigned has the state **offering**. Deployments that have the states **paused** or **scheduled** won't deploy content to devices.

4. Check that the device has scanned for updates and is scanning the Windows Update service.

   To learn more about scanning for updates, see Scanning updates.

5. **Feature updates only:** Verify that the device is successfully enrolled in feature update management by the deployment service. A device that's successfully enrolled is represented by an Azure AD device resource. That resource documents an update management enrollment for feature updates, and has no Azure AD device registration errors.

6. **Expedited quality updates only:** Check that the device has the Update Health Tools installed (available for Windows 10 version 1809 or later in the update described in KB 4023057 - Update for Windows 10 Update Service components, or a more recent quality update).

   The Update Health Tools are required for a device to receive an expedited quality update. The program's location on the device is *C:\Program Files\Microsoft Update Health Tools*. To verify its presence, view the installed programs list or run the following PowerShell script:

   ```
   PowerShell

   Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -Match
   "Microsoft Update Health Tools"}
   ```

The device is receiving an update that you didn't deploy

To troubleshoot this issue, follow these steps:

1. Check that the device is scanning the Windows Update service and not a different endpoint.

For example, if the device is scanning for updates from a WSUS endpoint, it might receive different updates. To learn more about scanning for updates, see Scanning updates.

2. **Feature updates only:** Check that the device is successfully enrolled in feature update management by the deployment service.

   A device that isn't successfully enrolled might receive different updates according to its feature update deferral period. A device that's successfully enrolled is represented by an Azure AD device resource. That resource documents an update management enrollment for feature updates, and has no Azure AD device registration errors.

References

- Log files created by Windows Update
- Windows Update troubleshooting
- Windows Update common errors and mitigation

.NET Framework 1.1 is not supported on Windows 7 nor Windows Server 2008 R2 and higher Operating Systems

Article • 09/23/2021 • 2 minutes to read

Microsoft .NET Framework version 1.1 is not supported on any version of Windows 7 or Windows Server 2008 R2 and higher Operating Systems.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2489698

Summary

While it might be possible to install .NET Framework 1.1 components on these operating systems, Microsoft will provide no level of support for these configurations.

More information

The Microsoft .NET Framework 1.1 is supported on operating systems up to and including Windows Vista.

More detailed information about newer .NET Framework Versions and OS Dependencies is available at the following web site:

.NET Framework versions and dependencies

You receive a 80072EE6 error code when you download an update from Windows Server Update Services

Article • 09/23/2021 • 2 minutes to read

This article helps resolve the 80072EE6 error code that occurs when you download an update from Windows Server Update Services.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2724184

Symptoms

Consider the following scenario:

- You have a computer that is running Windows
- You configure Windows Server Update Services (WSUS) over the Group Policy 'Specify intranet Microsoft update service location'.
- While trying to perform Windows Update, the update operation may fail. Additionally, you receive the following error code:

  > 80072EE6

Cause

This issue occurs if the URL under the Group Policy setting 'Specify intranet Microsoft update service location' is invalid.

For Example, `corp.contoso.com` or an IPaddress is invalid.

Resolution

To resolve this issue, follow steps below:

1. Click on Start and then type gpedit.msc.
2. Go to `Computer Configuration\Administrative Templates\Windows Components\Windows Update\`.

3. From the right-side pane, double-click on Specify intranet Microsoft update service location to open it.
4. Verify that the URL includes `http://` or `https://`. For Example, `http://corp.contoso.com` or `https://corp.contoso.comNote`.

More information

The above group policy setting lets you specify a server on your network to function as an internal update service. Automatic Updates will search this service for updates that apply to the computers on your network.

To use this setting, you must set two server name values: the server from which Automatic Updates detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server.

Analyze the log file entries that *SFC.exe* generates in Windows

Article • 09/23/2021 • 3 minutes to read

This article describes how to analyze the log files that the Microsoft Windows Resource Checker (*SFC.exe*) program generates in Windows.

Applies to: Windows Vista and later versions
Original KB number: 928228

Overview

You can use the *SFC.exe* program to help you troubleshoot crashes that occur in the user mode part of Windows. These crashes may be related to missing or damaged operating system files.

The *SFC.exe* program performs the following operations:

- It verifies that non-configurable Windows system files have not changed. Also, it verifies that these files match the operating system's definition of which files are expected to be installed on the computer.
- It repairs non-configurable Windows system files, when it is possible.

View the log file

The *SFC.exe* program writes the details of each verification operation and of each repair operation to the *CBS.log* file. Each *SFC.exe* program entry in this file has an **[SR]** tag. The *CBS.log* file is located in the *%windir%\Logs\CBS* folder.

> ⓘ **Note**
>
> The Windows Modules Installer service also writes to this log file. (The Windows Modules Installer service installs optional features, updates, and service packs.)

You can search for **[SR]** tags to help locate *SFC.exe* program entries. To perform this kind of search and to redirect the results to a text file, follow these steps:

1. Click **Start**, type *cmd* in the **Start Search** box, right-click **cmd** in the **Programs** list, and then click **Run as administrator**. If you are prompted for an administrator

password or for a confirmation, type your password, or click **Continue**.

2. Type the following command, and then press ENTER:

```
Console

findstr /c:"[SR]" %windir%\logs\cbs\cbs.log >sfcdetails.txt
```

The Sfcdetails.txt file includes the entries that are logged every time that the *SFC.exe* program runs on the computer.

Interpret the log file entries

The *SFC.exe* program verifies files in groups of 100. Therefore, there will be many groups of *SFC.exe* program entries. Each entry has the following format:

date time entry_type details

The following sample excerpt from a *CBS.log* file shows that the *SFC.exe* program did not identify any problems with the Windows system files:

```
Output

<date> <time>, Info CSI 00000006 [SR] Verifying 100 (0x00000064) components
<date> <time>, Info CSI 00000007 [SR] Beginning Verify and Repair
transaction
<date> <time>, Info CSI 00000009 [SR] Verify complete
<date> <time>, Info CSI 0000000a [SR] Verifying 100 (0x00000064) components
<date> <time>, Info CSI 0000000b [SR] Beginning Verify and Repair
transaction
<date> <time>, Info CSI 0000000d [SR] Verify complete
<date> <time>, Info CSI 0000000e [SR] Verifying 100 (0x00000064) components
<date> <time>, Info CSI 0000000f [SR] Beginning Verify and Repair
transaction
<date> <time>, Info CSI 00000011 [SR] Verify complete
<additional entries>
<additional entries>
<date> <time>, Info CSI 00000011 [SR] Verify complete
```

The following sample excerpt from a *CBS.log* file shows that the *SFC.exe* program has identified problems with the Windows system files:

```
Output

<date> <time>, Info CSI 00000006 [SR] Verifying 100 (0x00000064) components
<additional entries>
<additional entries>
```

```
<date> <time>, Info CSI 00000007 [SR] Beginning Verify and Repair
transaction
<date> <time>, Info CSI 00000008 [SR] Repairing corrupted file
[ml:520{260},l:108{54}]"??\E:\Program Files\Common Files\Microsoft
Shared\DAO"[l:20{10}]"dao360.dll" from store
<date> <time>, Info CSI 0000000a [SR] Verify complete
```

> **Note**
>
> Although the log file entry states that the *SFC.exe* program is repairing the changed file, no actual repair operation occurs when a file is verified.

The following list describes other messages that may be logged in the *SFC.exe* program entries of the *CBS.log* file after verification is completed.

- Entry 1: Cannot repair member file **file details**. For example:

  Output

  ```
  Cannot repair member file [l:14{7}]"url.dll" of Microsoft-Windows-IE-
  WinsockAutodialStub, Version = 6.0.5752.0, pA =
  PROCESSOR_ARCHITECTURE_INTEL (0), Culture neutral, VersionScope = 1
  nonSxS, PublicKeyToken = {l:8 b:31bf3856ad364e35}, Type neutral, TypeN
  ```

  This entry indicates that the file content does not match the operating system definition for the file. In this situation, the *SFC.exe* program cannot repair the file.

- Entry 2: Repaired file **file details** by copying from backup. For example:

  Output

  ```
  Repaired file \SystemRoot\WinSxS\Manifests\
  [ml:24{12},l:18{9}]"netnb.inf" by copying from backup
  ```

  This entry indicates that a problem exists with a file. The *SFC.exe* program can repair this file by copying a version from a private system store backup.

- Entry 3: Repairing corrupted file **file details** from store. For example:

  Output

  ```
  Repairing corrupted file [ml:520{260},l:36{18}]"??\C:\Windows\inf"
  [l:18{9}]"netnb.inf" from store
  ```

This entry indicates that a problem exists with a file. The *SFC.exe* program can repair this file by copying a version from the system store.

Automatic Updates can't download updates and event ID 16 is logged

Article • 09/23/2021 • 2 minutes to read

This article describes an issue where Automatic Updates can't download updates and event ID 16 is recorded in the system log.

Applies to: Windows 10 – all editions, Windows Server 2012 R2
Original KB number: 824208

Symptoms

When Automatic Updates tries to download updates, the download doesn't succeed, and Event ID 16 is recorded in the system log.

Cause

This behavior may occur if both of the following conditions are true:

- In your computer's Local Area Network (LAN) settings, the **Automatically detect settings** check box is selected.
- You can't ping the Web Proxy Auto-Discovery (WPAD) server by its Domain Name System (DNS) name. This behavior may occur if your computer's connection-specific DNS suffix doesn't match the DNS domain where the WPAD server's DNS entry is registered.

For your computer to automatically detect LAN settings, the WPAD server's DNS entry must be correctly configured, and a DNS query from your computer must successfully resolve the name `WPAD.mydomain.com`, where `mydomain.com` is the connection-specific DNS domain. If a DNS query from Automatic Updates can't resolve the name of the WPAD server, Automatic Updates can't use the WPAD server.

Resolution

To resolve this behavior, make sure that the WPAD server's DNS entry is correctly configured, and make sure that your computer's connection-specific DNS suffix matches the DNS domain where the WPAD server's DNS entry is registered.

Status

This behavior is by design.

More information

If you use Dynamic Host Configuration Protocol (DHCP), you can configure the **015 DNS Domain Name** option on the DHCP server to set the connection-specific DNS suffix of the client computers. After you configure this option, you must release and then renew the DHCP lease on the client computers.

To configure your DHCP server to set the connection-specific DNS suffix for its client computers, follow these steps:

1. If you use a Windows 2000 Server-based computer as your DHCP server, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **DHCP**.

   If you use a Windows XP-based computer as your DHCP server, click **Start,** click **Control Panel**, click **Performance and Maintenance**, click **Administrative Tools**, and then double-click **DHCP**.

   If you use a Windows Server 2003-based computer as your DHCP server, click **Start**, point to **Administrative Tools**, and then click **DHCP**.

2. Double-click the name of your server, right-click **Server Options**, and then click **Configure Options**.

3. In the **Available Options** list, click **015 DNS Domain Name**.

4. Under **Data entry**, in the **String value** box, type the connection-specific domain name that you want the client computers to use as their connection-specific DNS suffix.

   > ⓘ **Note**
   >
   > The connection-specific domain name must match the domain where the WPAD server's DNS entry is registered--for example, **mydomain.com**.

5. Click **OK**.

To release and to renew the DHCP lease on the client computers, and to confirm that the computer can resolve the WPAD server name, follow these steps:

1. From the command prompt, type `ipconfig /release`, and then press ENTER.
2. Type `ipconfig /renew`, and then press ENTER.
3. Type `ping WPAD.mydomain.com`, where `mydomain.com` is the connection-specific DNS domain, and then press ENTER.

> **Note**
>
> If the computer successfully resolves the name of the WPAD server, you see a series of messages that include the words "Reply from."

Cannot install the May 2019 update of Windows 10 on computers that run certain versions of AMD RAID drivers

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where the May 2019 update of Windows 10 cannot be installed on computers that run certain versions of AMD RAID drivers.

Applies to: Windows 10 - all editions
Original KB number: 4504107

Symptoms

When you install the May 2019 update on a Windows 10-based computer, the installation process stops, and you receive a message that resembles the following:

> AMD Ryzen™ or AMD Ryzen™ Threadripper™ configured in SATA or NVMe RAID mode.
> A driver is installed that causes stability problems on Windows. This driver will be disabled. Check with your software/driver provider for an updated version that runs on this version of Windows.

Cause

On computers that have AMD Ryzen or AMD Ryzen Threadripper processors, certain versions of AMD RAID drivers are not compatible with the Windows 10 May 2019 update. If a computer has these drivers installed and configured in RAID mode, it cannot install the May 2019 update of Windows 10. If you start the installation process, the process stops.

Version 9.2.0.105 and later versions of the AMD RAID drivers do not cause this issue. A computer that has these drivers installed can receive the May 2019 update.

For more information about this issue, see Article PA-260, Unable to proceed with installation or upgrade of Windows® 10 May 2019 Update with SATA or NVMe RAID on AMD Ryzen™ systems on the AMD website.

Resolution

To resolve this issue, download the latest AMD RAID drivers directly from AMD at X399 Drivers & Support. The drivers must be version 9.2.0.105 or a later version. Install the drivers on the affected computer, and then restart the installation process for the May 2019 update.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Third-party contact disclaimer

Microsoft provides third-party contact information to help you find additional information about this topic. This contact information may change without notice. Microsoft does not guarantee the accuracy of third-party contact information.

You can't use the ImageX.exe tool as a backup tool

Article • 09/23/2021 • 2 minutes to read

This article describes the reasons why you can't use the ImageX.exe tool as a backup tool for a Windows computer. The ImageX.exe tool ships as part of the Windows Automated Installation Kit (WAIK).

Applies to: Windows Server 2012 R2, Windows 7 Service Pack 1
Original KB number: 935467

Introduction

You can use the ImageX.exe tool to capture an operating system installation image on which you have run Sysprep (Sysprep.exe) from the Windows Preinstallation Environment (Windows PE). You can then deploy the operating system installation image on another computer.

Although the ImageX.exe tool may appear to be a mechanism to create an image of a computer for backup, there are some issues that prevent using the ImageX.exe tool as a supported backup mechanism.

Issues when you use imagex.exe as a backup mechanism

- Extended attributes are lost
- Sparse files on the system are captured and applied. However, the sparse files are no long sparse after they have been applied
- Symbolic links and junctions are automatically updated which in some scenarios such as Single Instance Storage(SIS) could lead to reparse points that contain NTFS file id's could be pointing to incorrect locations

Microsoft recommends you use Windows backup, Windows Server backup, or other tool designed specifically for backup to make a full system image backup.

Certificates are missing after you update a device to a newer version of Windows 10

Article • 03/04/2022 • 3 minutes to read

This article provides workarounds for an issue in which a device loses its system and user certificates after an operating system update.

Applies to: Windows 10, version 20H2; Windows 10, version 2004; Windows 10, version 1909; Windows 10, version 1903

Symptoms

You have a device that runs Windows 10, version 1809 or a later version. The device also has a latest cumulative update (LCU) that was released on September 16, 2020, or a later LCU. After you update the device to a later version of Windows, the device loses its system and user certificates.

Cause

This behavior might occur if the installation source or media that was used to update the device is out-of-date. The update doesn't include an LCU that was released on October 13, 2020, or later. The behavior typically affects managed devices in environments in which an update management tool such as Windows Server Update Services (WSUS) or Microsoft Endpoint Configuration Manager downloads updates and then distributes them to devices. It also affects devices that are updated by using outdated physical media or ISO images.

This behavior doesn't affect devices that use Windows Update for Business or that connect directly to Windows Update. Any device that connects to Windows Update should always receive the latest versions of the feature update, including the latest LCU, without any extra steps.

Workaround

To mitigate this issue, do one of the following:

- Download a new source image from the Microsoft Update Catalog or from the Volume Licensing Service Center to replace the previous source image. Then, use that image to update the device.
- Roll back the device to the previous Windows version, add the missing LCU to the update, and then reinstall the update.

> **ⓘ Important**
>
> - The rollback process does not affect your personal files, but it removes any apps and drivers that you installed after you installed the update. It also reverses any changes to settings that you made after you installed the update.
> - By default, you can roll back an update only within 10 days of installing it. You can change this time limit in a Command Prompt window by running the following command:
>
>   ```
>   Console
>
>   Dism /Online /Set-OSUninstallWindow /Value:<days>
>   ```
>
>   In this command, <*days*> is an integer between 2 and 60.

To roll back, follow these steps:

1. Select **Start** > **Settings** > **Update & Security** > **Recovery**.
2. Under **Go back to the previous version of Windows 10**, select **Get started**.

To add the latest LCU to the update source, follow these steps:

1. Mount the source ISO image, and then copy the *Install.wim* file to a writeable location.

   > **ⓘ Note**
   >
   > If the image has an *Install.esd* file instead of an *Install.wim* file, use the **Dism /Export-Image** command to convert the .esd file to a .wim file.

2. Go to Windows 10 update history to look up the correct LCU number for your system version.
3. Go to Microsoft Update Catalog, and then download the LCU.

> **Note**
>
> - If you're using WSUS to manage updates, see **WSUS and the Catalog Site**. This article describes how to use WSUS to download updates from the Microsoft Update Catalog.
> - If you are using Microsoft Endpoint Manager to manage updates, see **Software update management documentation**.

4. To add the LCU to the image, open an administrative Command Prompt window, and then run the following command:

```
Console

Dism /Add-Package /Image:"C:\Mount\Windows" /PackagePath="windows10.0-
kb4586781-x64_bd543ce012ec1695201cdb2d324a2206bd445132.msu"
/LogPath=C:\Mount\Dism.log
```

5. Review the list of packages that the `Dism` command produced, and verify that the list contains the package. To view the list, run the following command:

```
Console

Dism /Get-Packages /Image:<Path_to_Image>
```

> **Note**
>
> In this command, *<Path_to_Image>* is the path and filename of the image file.

6. Commit and unmount the image. To do this, run the following command:

```
Console

Dism /Unmount-Image /MountDir:<Path_to_Mount_Directory> /Commit
```

> **Note**
>
> In this command, *<Path_to_Mount_Directory>* is the path to the mounted image.

7. (Optional) Use the updated file to re-create the image. To do this, run the following command:

```
Console

Oscdimg –n –d –m “<Source>” “<Target.iso>”
```

> **Note**
>
> In this command, <*Source*> is the location of the files that you intend to build into an image, and <*Target.iso*> is the name of the ISO image file.

More information

- Add updates to a Windows image
- Add-WindowsPackage
- Modify a Windows image using DISM
- Oscdimg Command-Line Options

Command-line switches for Microsoft software update packages

Article • 04/12/2022 • 2 minutes to read

This article describes the consistent set of command-line switches that Microsoft is adopting for deploying packages that contain software updates.

Applies to: Windows 10 – all editions
Original KB number: 824687

Summary

Microsoft is adopting a consistent set of command-line switches that you can use to deploy packages that contain software updates, such as security updates, critical updates, and hotfixes. This article describes these new command-line switches and their behaviors.

> **Note**
>
> Packages that support these new command-line switches also support earlier command-line switches for backwards compatibility. However, usage of the earlier switches should be discontinued as this support may be removed in future software updates.

For additional information about command-line switches that are used by Windows software update packages, click the following article number to view the article in the Microsoft Knowledge Base:

262841 Command-line switches for Windows software update packages

For additional information about command-line switches used by Windows Installer, visit the following Microsoft Web site:

Command-Line Options

More information

Microsoft is adopting the following command-line switches for software update packages:

- /help; /h; /? - Displays a dialog box that shows the correct usage of the Setup command, including a list of all its command-line switches and their behaviors. You can display this help information in the command-line interface (CLI) or the graphical user interface (GUI). If you use any command-line switch incorrectly, this help switch is invoked and the correct usage is displayed. The dialog box also provides references to more online information.

- /quiet - Runs the Setup program or the removal program in "quiet" mode. The program doesn't prompt the user with any messages. The program enters all messages in a log file. By default, the program restarts the computer with no prompt or warning if the process requires a restart for the changes to take effect. To change the default restart behavior, use a different restart mode.

- /passive - Runs the Setup program or the removal program in "passive" mode. The program doesn't prompt the user with any error messages. The user sees a progress bar that indicates that the installation or the removal is occurring. The user can't cancel the installation or the removal. By default, the program invokes the /warnrestart switch. If the program is installing multiple updates, the progress bar indicates the progress of the installation or the removal for each update.

- /norestart - Doesn't restart the computer after the installation or the removal, even if the process requires a restart for the changes to take effect.

- /forcerestart - Restarts the computer after the installation or the removal, even if the process doesn't require a restart for the changes to take effect. Restarting forces programs that are running to close.

- /warnrestart[:**x**] - Invokes a dialog box that warns the user that a restart will occur in **x** seconds (in 30 seconds if no value is specified). For example, to warn that a restart will occur in 60 seconds, type /warnrestart:60. The dialog box contains a **Cancel** button and a **Restart Now** button. If the user clicks **Cancel**, the computer isn't restarted.

- /promptrestart - Prompts the user that the computer must be restarted for the changes to take effect. The user can select whether to restart the computer.

- /uninstall - Removes the package.

- /log - Enables the user to define the path for the local log file. This switch invokes the default logging behavior.

- /extract - Enables you to extract the installation files to a specified folder.

Command-line switches supported by a software installation package, an update package, or a hotfix package created with Microsoft Self-Extractor

Article • 03/24/2022 • 2 minutes to read

This article describes the command line switches supported by a software installation package, an update package, or a hotfix package that's created by using Microsoft Self-Extractor.

Applies to: Windows 10 - all editions
Original KB number: 912203

Summary

A Self-Extractor package is a self-extracting executable (.exe) file. You can run the .exe file to install the package. To run the .exe file, use one of the following methods:

- Double-click the .exe file.
- Run the .exe file from a command line.

Run Self-Extractor packages from a command line

If you run the .exe file from a command line, several switches may be available for use in the package.

> ⓘ **Note**
>
> Not all switches may be available in all packages.

To determine which switches are available in the package, use one of the following Help switches:

- `/?`
- `/h`
- `/help`

The following table lists the command-line switches that are supported by Microsoft Self-Extractor.

Switch	Description
`/extract:[path]`	Extracts the content of the package to the path folder. If a path isn't specified, then a **Browse** dialog box appears.
`/log:[path to log file]`	Enables verbose logging for the update installation. Besides the path information, the file name must be included. Because the command doesn't create a folder that doesn't exist, only an existing folder name should be provided. Besides the file name that is specified, a separate log file will be created for each .msi file that is run.
`/lang:lcid`	Sets the user interface to the specified locale when multiple locales are available in the package.
`/quiet`	Runs the package in silent mode.
`/passive`	Runs the update without any interaction from the user.
`/norestart`	Prevents prompting of the user when a restart of the computer is needed.
`/forcerestart`	Forces a restart of the computer as soon as the update is finished.
`/?`, `/h`, `/help`	Shows this help message.

DISM /Apply-Image command fails with error code 5 (ERROR_ACCESS_DENIED)

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where `DISM /Apply-Image` command fails with error code 5 (ERROR_ACCESS_DENIED).

Applies to: Windows 10 - all editions
Original KB number: 3179598

Symptoms

Consider the following scenario:

- You have a Windows 10 image.
- You enable the Windows Subsystem for Linux (WSL) feature.
- You download and install Ubuntu package by using the command that's documented here.
- You capture the Windows 10 image by using the `DISM /Capture-Image` command.
- You try to apply the captured Windows 10 image by using the `DISM /Apply-Image` command.

In this scenario, the `DISM /Apply-Image` command fails with error code 5 (ERROR_ACCESS_DENIED).

Cause

The files that are installed by the Ubuntu package may cause `DISM /Apply-Image` to fail.

Workaround

Do not download and install the Ubuntu package before you capture the Windows 10 image by using the `DISM /Capture-Image` command. The Ubuntu package can be downloaded and installed after the Windows 10 image is applied to a device. You can install the Ubuntu package by following the steps in this installation guide.

More Information

For more information about Windows Subsystem for Linux, see Frequently Asked Questions.

For more information about DISM imaging commands, see DISM Image Management command-line options.

How to download updates that include drivers and hotfixes from the Windows Update Catalog

Article • 08/31/2022 • 5 minutes to read

This article discusses how to download updates from the Windows Update Catalog.

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 323166

Introduction

The Windows Update Catalog offers updates for all operating systems that we currently support. These updates include the following:

- Device drivers
- Hotfixes
- Updated system files
- New Windows features

We guide you through the steps to search the Windows Update Catalog to find the updates that you want. Then, you can download the updates to install them across your home or corporate network of Microsoft Windows-based computers.

We also discuss how IT Professionals can use Software Update Services, such as Windows Update and Automatic Updates.

> **ⓘ Important**
>
> This content is designed for an advanced computer user. We recommend that only advanced users and administrators download updates from the Windows Update Catalog. If you are not an advanced user or an administrator, visit the following Microsoft Web site to download updates directly:
> **Windows Update: FAQ**

Steps to download updates from the Windows Update Catalog

To download updates from the Windows Update Catalog, follow these steps:

Step 1: Access the Windows Update Catalog

To access the Windows Update Catalog, visit the following Microsoft Web site:
Windows Update Catalog

To view a list of frequently asked questions about Windows Update Catalog, visit the following Microsoft Web site:
Microsoft Update Catalog Frequently Asked Questions

Step 2: Search for updates from the Windows Update Catalog

To search for updates from the Windows Update Catalog, follow these steps:

1. In the **Search** text box, type your search terms. For example, you might type *Windows Vista Security*.
2. Click **Search**, or press **Enter**.
3. Browse the list that is displayed to select the updates that you want to download.
4. Click **Download** to download the updates.
5. To search for additional updates to download, repeat steps 2a through 2d.

Step 3: Download updates

To download updates from the Windows Update Catalog, follow these steps:

1. Click the **Download** button under **Search** box.
2. Click the updates link on the pop-up page and **Save** to the default path, or right-click the link and select **Save target as** to the specified path. You can either type the full path of the folder, or you can click **Browse** to locate the folder.
3. Close the **Download** and the **Windows Update Catalog** Window.
4. Find the location that you specified in step 3b.

> **Note**

If you have downloaded device drivers for installation, go to "Installing Drivers."

5. Double-click each update, and then follow the instructions to install the update. If the updates are intended for another computer, copy the updates to that computer, and then double-click the updates to install them.

If all the items that you added to the download list are installed successfully, you are finished.

If you want to learn about additional update services, please see the "Software Update Services for IT Professionals" section.

Installing drivers

1. Open a command prompt from the **Start** menu.
2. To extract the driver files, type the following command at the command prompt, and then press **Enter**:

```
Console

expand <CAB FILE NAME> -F:* <DESTINATION>
```

3. To stage the driver for plug and play installation or for the Add Printer Wizard, use PnPutil Software Update Services for IT Professionals.

> **Note**
>
> To install a cross-architecture print driver, you must already have installed the local architecture driver, and you will still need the cross-architecture copy of Ntprint.inf from another system.

Software Update Services for IT Professionals

For general information about Software Update Services, visit the following Microsoft Web site:
Overview of Windows as a service

Windows Update

IT Professionals can use the Windows Update service to configure a server on their corporate network to provide updates to corporate servers and clients. This functionality can be useful in environments where some clients and servers do not have access to the Internet. This functionality can also be useful where the environment is highly managed, and the corporate administrator must test the updates before they are deployed.

For information about using Windows Update, visit the following Microsoft Web site: Windows Update: FAQ

Automatic Updates

IT Professionals can use the Automatic Updates service to keep computers up to date with the latest critical updates from a corporate server that is running Software Update Services.

Automatic Updates works with the following computers:

- Microsoft Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server (Service Pack 2 or later versions)
- Windows XP Professional
- Windows XP Home Edition computer

For more information about how to use Automatic Updates in Windows XP, click the following article number to view the article in the Microsoft Knowledge Base: 306525 How to configure and use Automatic Updates in Windows XP

Troubleshooting

You may experience one or more of the following issues when you use Windows Update or Microsoft Update:

- You may receive the following error message:

  > Software update incomplete, this Windows Update software did not update successfully.

- You may receive the following error message:

  > Administrators Only (-2146828218) To install items from Windows Update, you must be logged on as an administrator or a member of the Administrators

> group. If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.

For more information about this issue, click the following article number to view the article in the Microsoft Knowledge Base: 316524 You receive an "Administrators only" error message when you try to visit the Windows Update Web site or the Microsoft Update Web site

- You may be unable to view the Windows Update site or the Microsoft Update site if you connect to the Web site through an authenticating Web proxy that uses integrated (NTLM) proxy authentication.

Similar problems and solutions

You can visit the Microsoft Web sites in the following sections for more information:
Windows Update troubleshooting

Installing multiple updates with only one restart

The hotfix installer that is included with Windows XP and with Windows 2000 post-Service Pack 3 (SP3) updates includes functionality to support multiple hotfix installations. For earlier versions of Windows 2000, the command-line tool that is named "QChain.exe" is available for download.

For more information about how to install multiple updates or multiple hotfixes without restarting the computer between each installation, click the following article number to view the article in the Microsoft Knowledge Base:
296861 How to install multiple Windows updates or hotfixes with only one reboot

Microsoft security resources

For the latest Microsoft security resources such as security tools, security bulletins, virus alerts, and general security guidance, see Security documentation.

For more information about the Microsoft Baseline Security Analyzer tool (MBSA), see What is Microsoft Baseline Security Analyzer and its uses?.

The Microsoft Download Center

For more information about how to download files from the Microsoft Download Center, click the following article number to view the article in the Microsoft Knowledge

Base:

119591 How to obtain Microsoft support files from online services

Product-specific download pages

Internet Explorer

For Internet Explorer downloads, visit the following Microsoft Web site:
Internet Explorer Downloads

Windows Media Player

For Windows Media Player downloads, visit the following Microsoft Web site:
Windows Media Player

Office Updates

For Office updates, visit the following Microsoft Web site:
Install Office updates

Error 403 (Access Denied/Forbidden) occurs when you connect to Windows Update

Article • 11/26/2021 • 2 minutes to read

This article provides a solution to an error 403 that occurs when you access Windows Update.

Applies to: Windows 10 - all editions
Original KB number: 245142

Symptoms

When you try to access the Windows Update website, you receive the following error message:

> Error 403: Access Denied/Forbidden

Cause

This issue occurs for any of the following reasons:

- You're running personal firewall software or some other security, download assistant, or web accelerator software.
- The Windows Update site control is missing or is damaged on your computer.
- The Hosts file is damaged or contains incorrect information.
- There are missing or damaged Internet Explorer files that display the script on the page.

Resolution

To resolve this issue, use one of the following procedures based on what's causing the issue. If you don't know what's causing the error message, use these resolutions in the order that they're listed. For example, if the first resolution doesn't solve the issue, continue to the next resolution.

Disable security, download assistant, or web accelerator software

1. Microsoft has verified that the kinds of software programs in the following list contribute to **Unauthorized** or **Access Denied/Forbidden** errors. Disable any third-party software that fits one of the following descriptions:

    - Ad removal programs
    - Web accelerators
    - Download assistants
    - Security software
    - Antivirus software

2. Try to connect to the Windows Update site by going to Microsoft Update.

3. If you still can't connect, try the next resolution.

Reset the Hosts file to the default

For information about how to reset the Hosts file to the default Hosts file, see How can I reset the Hosts file back to the default?.

Install a new scripting engine

> **Note**
>
> These steps only apply to computers that are running Windows XP or earlier versions of Windows.

1. Go to the Microsoft Download Center.

2. Click the Update symbol next to the update for your version of Windows.



3. Click **Download** (on the right side of the page).

4. Click **Save to Disk**, and then save the file to the default location.

5. On your desktop, double-click the STE56en.exe icon (for Microsoft Windows 98, Microsoft Windows Millennium Edition, and Windows NT) or double-click the

Scripten.exe icon (for Microsoft Windows 2000 and Windows XP).

6. After the installation is complete, you can remove STE56en.exe or Scripten.exe file from your Desktop. To do so, right-click the icon, and then click **Delete**.
7. Restart your computer, and then go to the Windows Update website.

> ⓘ **Note**
>
> Some Internet accelerators change the Hosts file. To resolve this issue, rename the file.

DISM command fails with error code 87 when you try to apply a Windows 10 image

Article • 06/21/2022 • 2 minutes to read

This article provides a solution to the error 87 that occurs when you try to apply a Windows 10 image.

Applies to: Windows 10 - all editions
Original KB number: 3082581

Symptoms

Consider the following scenario:

- You have a Windows 10 image.
- Windows has Compact OS compression enabled on some files.
- You have an earlier version of DISM (that is, a version from Windows 8.1 or from an earlier version of Windows).
- You try to apply the Windows 10 image by using the DISM /Apply-Image command.

In this scenario, the command fails with error code 87. Additionally, the DISM log file shows the following error message:

> Error DISM DISM WIM Provider: PID=1804 [RestoreReparsePoint:(1332) -> ioctl: setting reparse point tag failed]
>
> C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Runt0d283adf#\9766308db336f6018797df6128270717\System.Runtime.WindowsRuntime.ni.dll (HRESULT=0x80070057) - CWimManager::WimProviderMsgLogCallback

Cause

To apply a Windows 10 image, you must use the Windows 10 version of DISM. This version requires the Wofadk.sys filter driver.

> ⓘ **Note**

The Wofadk.sys filter driver is included in the Windows 10 Assessment and Deployment Kit (ADK). The driver must be installed and configured to be used with Window 10 DISM when the command runs on an earlier version of Windows host or Windows Preinstallation Environment (Windows PE).

Resolution

Use the Windows 10 version of DISM with Wofadk.sys filter driver. For more information, see DISM Supported Platforms and Copy DISM to Another Computer.

More information

For more information about Compact OS compression, see Compact OS, single-instancing, and image optimization. In that article, see the "To deploy Windows using a WIM file section for more information about how to deploy Windows by using a WIM file.

Error message when installing RSAT: This update is not applicable to your computer

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an error that occurs when you install the Remote Server Administration Tools (RSAT).

Applies to: Windows 7 Service Pack 1
Original KB number: 2517239

Symptoms

When installing the Remote Server Administration Tools for Windows 7 (RSAT), you may receive the following error message:

> "This update is not applicable to your computer"

Cause

This error will occur if you attempt to install RSAT after installing Service Pack 1 for Windows 7. The RSAT tools are designed for the RTM version of Windows 7 and are not compatible with Service Pack 1. However, Service Pack 1 includes updated components for RSAT, so if RSAT is installed before Service Pack 1, the issue will not occur and the components will be updated automatically.

Resolution

Install RSAT tools before installing Service Pack 1 for Windows 7. If Service Pack 1 for Windows 7 is already installed, it can be uninstalled and then reinstalled after the RSAT tools are installed.

More information

Microsoft has confirmed this to be by design, as RSAT was designed for Windows 7 RTM version. A newer version of RSAT is slated to be released in the future.

"Error: 0x8004005" or "Error: 0x800C0005" error messages when you scan for updates

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to error messages when you scan for updates.

Applies to: Windows 10 - all editions
Original KB number: 843499

Symptoms

When you visit the Windows Update Web site and then select **Scan for updates**, the result of the scan is zero percent. Additionally, you may receive one of the following error messages:

> Error: 0x800C0005

> Error: 0x8004005

Cause

This behavior may occur if certain dynamic-link library files (.dll files) aren't registered correctly or if there's a firewall between the computer and the Internet that doesn't allow HTTPS (SSL) connections.

Resolution

To resolve this behavior, use the `regsvr32` command to register several .dll files:

1. Select **Start**, select **Run**, type cmd in the **Open** box, and then select **OK.**
2. At the command prompt, type the following commands. Press **ENTER** after each line:

```
Console

regsvr32 Softpub.dll
regsvr32 Wintrust.dll
```

```
regsvr32 Initpki.dll
```

3. Select **OK**.

4. Restart your computer.

Fix errors found in the CheckSUR.log

Article • 09/23/2021 • 3 minutes to read

This article describes how to resolve servicing corruption that the System Update Readiness tool (CheckSUR) finds but cannot correct on its own. Output from the tool is recorded in the %WinDir%\Logs\CBS\CheckSUR.log file.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2700601

> ⓘ **Note**
>
> Make sure you download and run the most recent version of CheckSUR.exe because the tool is updated periodically. To to this, see **Fix Windows Update errors by using the DISM or System Update Readiness tool**.

Use the CheckSur log

To use the CheckSur log, follow these guidelines:

- If CheckSUR fixed all the errors that it found, the CheckSUR log shows the following information:

  ```
  Summary:
  Seconds executed: 100
  Found 10 errors
  Fixed 10 errors
  ```

  In this scenario, you should no longer have any servicing corruption on your computer. If you are still experiencing errors, you have to troubleshoot the specific error message to find the root cause of the failure.

- If you receive an **Unavailable repair files** message, this indicates that some of the inconsistent files that the tool found cannot be fixed. This is because the tool does not carry the correct versions of the replacement files. After this message appears, the CheckSUR.log shows information that resembles the following:

  ```
  Summary:
  Seconds executed: 264
  Found 3 errors
  ```

> CBS MUM Missing Total Count: 3
> Unavailable repair files:
>
> servicing\packages\Package_for_KB958690_sc_0~31bf3856ad364e35~amd64~~6.0.1.6.mum
> servicing\packages\Package_for_KB958690_sc~31bf3856ad364e35~amd64~~6.0.1.6.mum
> servicing\packages\Package_for_KB958690~31bf3856ad364e35~amd64~~6.0.1.6.mum
> servicing\packages\Package_for_KB958690_sc_0~31bf3856ad364e35~amd64~~6.0.1.6.cat
> servicing\packages\Package_for_KB958690_sc~31bf3856ad364e35~amd64~~6.0.1.6.cat
> servicing\packages\Package_for_KB958690~31bf3856ad364e35~amd64~~6.0.1.6.cat
> winsxs\manifests\x86_microsoft-windows-servicingstack_31bf3856ad364e35_6.0.6002.18005_none_0b4ada54c46c45b0.manifest
> winsxs\manifests\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.0.6002.18005_none_676975d87cc9b6e6.manifest

To resolve this issue, follow these steps:

1. Download the package that contains the missing files. For this example, you would download Windows6.0-KB958690-x64.msu.
2. In the `%SYSTEMROOT%\CheckSUR` folder, create a folder that is named Packages. Copy the Windows6.0-KB958690-x64.msu to the `%SYSTEMROOT%\CheckSUR\Packages` folder.
3. Rerun CheckSUR.
4. If the source package of the missing files is not obvious, you will have to get the files from another computer. Make sure the computer from which you copy the filhates uses the same OS version and system architecture as the computer that you are working on.
5. Copy the files to the `%WinDir%\Temp\CheckSUR` folder of the corrupted computer in the following subdirectory format, and then rerun CheckSUR:
   - Put all files of type *.mum and *.cat into the `%WinDir%\Temp\CheckSUR\Packages` folder.
   - Put all files of type *.manifest into the `%WinDir%\Temp\CheckSUR\Manifests` folder.

- If you see a **Payload File Missing** message, this indicates that the required binary file is not available. This means that the issue is not fixed. The CheckSUR.log shows the following information:

  > Summary:
  > Seconds executed: 100
  > Found 3 errors
  > Fix 1 errors
  > CSI Payload File Missing Total count: 3
  > Fix CSI Payload File Missing Total Count: 1
  >
  > (f) CSI Payload File Missing 0x00000000 admparse.dll x86_microsoft-windows-ie-adminkitmostfiles_31bf3856ad364e35_6.0.6000.16386_none_abfb5fd109dad8b8 servicing_31bf3856ad364e35_6.0.6000.16386_none_23ddbf36a8a961bc
  > (f) CSI Payload File Missing 0x00000000 bootmgr x86_microsoft-windows-b..re-bootmanager-pcat_31bf3856ad364e35_6.0.6000.16386_none_c0f2f087b6457236
  > (fix) CSI Payload File Missing 0x00000000 bootmgr x86_microsoft-windows-b..re-bootmanager-pcat_31bf3856ad364e35_6.0.6000.16386_none_c0f2f087b6457236
  > (f) CSI Payload File Missing 0x00000000 winload.exe x86_microsoft-windows-b..environment-windows_31bf3856ad364e35_6.0.6000.16386_none_6701d52e8fdf8d45

  To resolve this issue, follow these steps:

  1. Find out which payload files are missing. To do this, examine the CheckSUR log. Identify any lines that have an **(f)** entry that is not followed by **(fix)**. In the previous example, there are two payload files that were not fixed.
  2. Copy these files from another computer. Make sure the computer from which you copy files uses the same OS version and system architecture as the computer that you are working on.
  3. Paste the files into the appropriate subfolder under `%windir%\winsxs`.

Before you put the files into the indicated locations, you may have to grant yourself permissions to edit the folder contents. To do this, open an elevated Command Prompt window, and run the following commands:

Console

```
takeown /f <Path_And_Name>
icacls <Path_And_Name> /grant Administrators:F
```

> **Note**
>
> In these commands, <Path_And_Name> represents the name of the file or folder that you are targeting. For example, you might target the following folder: `C:\Windows\winsxs\x86_microsoft-windows-ie-adminkitmostfiles_31bf3856ad364e35_6.0.6000.16386_none_abfb5fd109dad8b8`

The following commands take ownership of this folder, grant Full Control of the folder to the Administrators group, and then replace the admparse.dll file:

Console

```
takeown /f C:\Windows\winsxs\ x86_microsoft-windows-ie-
adminkitmostfiles_31bf3856ad364e35_6.0.6000.16386_none_abfb5fd109dad8b8
icacls C:\Windows\winsxs\x86_microsoft-windows-ie-
adminkitmostfiles_31bf3856ad364e35_6.0.6000.16386_none_abfb5fd109dad8b8
/grant Administrators:F copy C:\Temp\admparse.dll
c:\Windows\winsxs\x86_microsoft-windows-
ieadminkitmostfiles_31bf3856ad364e35_6.0.6000.16386_none_abfb5fd109dad8b8\ad
mparse.dll
```

Skype for Microsoft Update

Article • 10/27/2021 • 2 minutes to read

This article describes how to keep Skype updated through Microsoft Update and through the Upgrade function in Skype.

Applies to: Windows 10 - all editions
Original KB number: 2876229

Summary

Skype releases new versions of Skype for Windows throughout the year. To help you stay current with new functionality and features of the Skype experience, Skype is available through Microsoft Update.

Skype includes the following:

- Chat every day with free instant messages.
- Share photos and see them inline, right in the chat.
- See your family come together over a free group video call.
- Switch between calling and messages - or do both at the same time.
- Make low-cost calls and text messages to mobiles and landlines

To make it simple and fast for Skype users to upgrade to the latest version of Skype for Windows, we've integrated Skype into Microsoft Update. If you have Skype installed on your PC already, either directly from Skype website or through a preinstalled version on your PC, you'll receive the latest version of Skype through Microsoft Update.

More information

To check whether Skype is already installed on your PC, follow these steps:

1. Select **Start**, select **Run**, type *regedit* in the **Open** window, and then select **OK**.
2. In the navigation pane of the **Registry Editor** window, look for the following registry key: `HKEY_CURRENT_USER\Software\Skype\Phone`
3. If the registry key exists, select the `Phone` folder. If the registry key doesn't exist, Skype isn't installed on the computer.
4. In the main pane of the **Registry Editor** window, you should see an entry that is named `SkypePath`. The value in the **Data** column will tell you where Skype is

installed on the computer. If the `SkypePath` entry doesn't exist, go to step 5.

5. If the `SkypePath` key doesn't exist, look for the following registry key, and then repeat steps 3 and 4: `HKEY_LOCAL_MACHINE\Software\Skype\Phone`

> **Note**
>
> If the `HKEY_CURRENT_USER\Software\Skype\Phone` key doesn't exist, and if the `HKEY_LOCAL_MACHINE\Software\Skype\Phone` key does exist, Skype was installed from an administrator account but was not used from the current account. If neither key exists, Skype is not installed on the computer.

If you're planning to upgrade from an earlier version of Skype for Windows, you can learn more about the updates on the Skype blog.

You can obtain the update in two ways:

- Through Microsoft Update.
- Through the Upgrade function in the Skype application. To use the Upgrade function, follow these steps:

    1. On the menu bar, select **Help**, and then select **Check for Updates**.
    2. After you check the version, select **Download**, and then select **Upgrade**.

> **Note**
>
> Skype will automatically be updated only on PCs on which Skype is already installed. Skype will not automatically be updated on any PC that doesn't already have Skype installed.

How can I install the latest version of Skype for Windows?

To install Skype for Windows, follow these steps:

1. Download the latest version from the Skype website.
2. Select **Run** to run Skype directly from your browser.
3. Follow the steps in the setup wizard to complete the installation.
4. Start Skype, and then sign in by entering a Microsoft Account user name and password.

How to downgrade from Windows 8

Article • 12/06/2021 • 5 minutes to read

Applies to: Windows 8
Original KB number: 2832566

Summary

Your ability to downgrade Windows 8 to an earlier version of Windows depends both on the version of Windows 8 that you've and on the method by which you obtained Windows 8. Not all Windows editions provide downgrade rights. If you do have downgrade rights and decide to use them, you continue to keep the license and rights of use for your original version and may "upgrade" back at any time.

More information

The primary methods of obtaining Windows 8 are as follows:

- You can buy a retail version of Windows 8 and install it as an upgrade on a PC that is running Windows XP, Windows Vista, or Windows 7.
- You can buy and install a personal-use license of Windows 8 System Builder.
- You can buy a PC that has Windows 8 preinstalled from an OEM.
- You can buy a Volume Licensing agreement and then install a Windows 8 Pro upgrade or Windows 8 Enterprise on a PC that is running a qualifying operating system.

Downgrade rights

The downgrade rights for each scenario that is mentioned in the previous section are as follows.

For a retail version of Windows 8

There are no downgrade rights for retail versions of Windows 8. If you upgraded Windows by using a retail version of Windows 8, you have to reinstall your earlier version of Windows by using the recovery or installation media that was included with your PC.

If you don't have recovery media, you can create it before you upgrade from a recovery partition on your PC by using software that is provided by your PC manufacturer. Check the support section of your PC manufacturer's website for more information. Make sure that you have this recovery disk before you upgrade, because you won't be able to use the recovery partition to create a recovery disk after you install Windows 8.

For more information about how to start your PC from recovery media, see Create installation media for Windows.

For a personal-use license of Windows 8 System Builder

If you installed Windows 8 by purchasing and installing Windows 8 System Builder yourself, there are no downgrade rights. It's governed by the personal-use Microsoft Software License Terms for the product. The process for downgrading to an earlier version of Windows is the same as it is for a retail version of Windows 8. That is, you have to buy or have previously bought a product key for the earlier version of Windows and then install that version by using the recovery or installation media.

For a PC that has Windows 8 preinstalled by an OEM

OEM downgrade rights apply to only Windows 8 Pro and allow for downgrades for up to two earlier versions (to Windows 7 Professional and to Windows Vista Business).

How to downgrade your PC

Your OEM will have the best information about how to downgrade your specific PC and in some cases may decide to send you installation media or a PC that has the operating system downgrade already installed.

> **Note**
>
> Neither Microsoft nor the OEM is obligated to provide media for the downgrade.

To do the downgrade on your PC yourself, follow these steps:

1. Change the settings so that the computer starts in legacy BIOS mode.

   > **Note**
   >
   > If you want to upgrade back to Windows 8 Pro later and want full Windows 8 Pro functionalities, you must change the BIOS setting back to native UEFI

mode before you install Windows 8 Pro. This is also true if you upgrade to Windows 8 Pro on a PC that was sold to you with the downgrade preinstalled.

2. Some OEMs pre-inject the product key for Windows 7 Professional or Windows Vista Business into the BIOS for just such an occasion. If your OEM did it on your PC, you have to take only one of the following actions:

    - Install Windows 7 Professional or Windows Vista Business by using the recovery media for that version of Windows that was provided by the same OEM. Your system will activate automatically by using the product key that was injected into the BIOS.
    - Install Windows 7 Professional or Windows Vista Business by using a genuine copy of the installation media for that version of Windows. Your system will activate automatically by using the product key that was injected into the BIOS.
    - Activate your copy of Windows 7 Professional or Windows Vista Business by using a Volume License Key Management Service (KMS). The KMS will be able to activate your system by checking the preinstalled product key.

3. If your OEM hasn't injected your product key into the BIOS on your PC, follow these steps:
    a. Obtain genuine Windows 7 Professional or Windows Vista Business installation media and the corresponding product key. You may have to buy a full-package product copy of the Windows downgrade from a retailer.
    b. Insert the media for the downgrade version of Windows into the PC, and then follow the installation instructions.
    c. Type the product key when you're asked to do this. If the software was previously activated, you can't activate it online. In this case, the local Activation Support telephone number will be displayed. Call the number, and explain the circumstances. When it's determined that you have an eligible Windows license, the customer service representative will provide a single-use activation code to activate the software. Microsoft doesn't provide a full product key in this scenario.

How to downgrade by using a Volume Licensing agreement for Windows 8 Pro Upgrade or Windows 8 Enterprise

Volume Licensing provides the greatest flexibility as to downgrade rights. Volume Licensing allows for downgrades to additional earlier versions and editions. The

following table summarizes downgrade eligibility. There are no downgrade rights to Windows 7 Ultimate.

Version Downgrading to	OEM Preinstall	Volume Licensing	
	Windows 8 Pro	Windows 8 Pro upgrade without Software Assurance	Windows 8 Enterprise with Software Assurance
Windows 7 / Vista Enterprise			■
Window 7 Professional	■	■	■
Windows Vista Business	■	■	■
Windows XP Pro		■	■
Windows 2000 Professional		■	■
Windows 95 / 98 / NT		■	■

> ⓘ **Note**
>
> A Windows 8 customer who has multi-language functionality cannot downgrade to Windows 7 Pro or to Windows XP Pro. This is because the multi-language functionality is exclusive to Windows 7 Enterprise and is not available for a Professional edition.

The Microsoft Volume Licensing Service Center (VLSC) provides download access to versions of Windows through the end of those versions' support life cycle.

> ⓘ **Note**
>
> In addition to the VLSC download software access, all Volume Licensing customers may decide to buy physical media (CD/DVD) copies of their licensed software through their Microsoft reseller.

If you legally obtained physical media (CD/DVD) of earlier Microsoft products that your organization is currently licensed to use through downgrade rights, you can use these prior software versions at your discretion.

How to get an update through Windows Update

Article • 09/23/2021 • 2 minutes to read

This article describes how to obtain updates from Windows Update in Windows 7, Windows 8.1 and Windows Server 2012 R2.

Applies to: Windows 8.1, Windows Server 2012 R2, Windows 7 Service Pack 1
Original KB number: 3067639

Detailed steps for Windows 8.1 and Windows Server 2012 R2

1. Swipe in from the right edge of the screen, and then tap **Search**. Or, if you are using a mouse, point to the lower-right corner of the screen, and then select **Search**.
2. In the search box, type *Windows Update*, and then tap or select **Windows Update**.
3. In the details pane, select **Check for updates**, and then wait while Windows looks for the latest updates for your computer.
4. If you see a message telling you that important or optional updates are available, or telling you to review important or optional updates, select the message to view the updates to install.
5. In the list, select the check box for the updates that you want to install under **Important** or **Optional**, and then tap or select **Install**.

Detailed steps for Windows 7 Service Pack 1

1. Click **Start**, type update in the search box, in the list of results, click **Windows Update**.
2. In the details pane, click **Check for updates**, and then wait while Windows looks for the latest updates for your computer.
3. If you see a message telling you that important or optional updates are available, or telling you to review important or optional updates, click the message to view the updates to install.

4. In the list, select the check box for the updates that you want to install, click **OK**, and then click **Install updates**.

Reference

See the frequently asked questions for Windows Update.

How to keep your Windows computer up to date

Article • 09/23/2021 • 3 minutes to read

This article helps your computer obtain the latest updates to protect the computer and make it run smoothly.

Applies to: Windows XP
Original KB number: 311047

Install high priority updates

Microsoft Update is the online extension of Windows that helps you keep your computer up to date. Microsoft Update includes updates from Windows Update and from Office Update, in addition to updates for other Microsoft products and for third-party device drivers. Use Microsoft Update to install updates for your computer's operating system, software, and hardware.

New content is added to the site regularly so that you can obtain recent updates and fixes to help protect your computer and to keep it running smoothly. To use the Microsoft Update site to install all critical updates for your computer, follow these steps:

1. Connect to the Internet, and then start Internet Explorer.
2. On the **Tools** menu, select **Windows Update**.
3. If Microsoft Update is not installed, select **Microsoft Update**. Otherwise, go to step 7.
4. On the **Try Microsoft Update today** Web page, select **Start Now**, and then select **Continue** on the **Review the license agreement** web page.
5. In the **Security Warning** dialog box, select **Install** to install Microsoft Update.
6. On the **Welcome to Microsoft update** web page, select **Check for Updates**
7. On the **Keep your computer up-to-date** web page, select **Express** to install high priority updates.
8. On the **Review and Install Updates** web page, select **Install Updates**, and then follow the instructions on the screen to complete the installation.

9. After you install the high priority updates, you can repeat these steps to install other updates. To do this, select **Custom** on the **Keep your computer up-to-date** web page. Then, you can select updates from the sections that are listed on the navigation pane.

Automatic Updates feature

You can also use the Automatic Updates feature to install updates. By using Automatic Updates, you do not have to visit the Microsoft Update Web site to scan for updates. Instead, Windows automatically delivers them to your computer.

Automatic Updates recognizes when you are online, and searches for updates from the Windows Update Web site. An icon appears in the notification area at the far right of the taskbar every time that new updates are available. You can specify how and when you want Windows to update your computer. For example, you can configure Windows to automatically download and to install updates on a schedule that you specify. Or you can have Windows notify you when it finds updates that are available for your computer, and then download the updates in the background. This enables you to continue to work uninterrupted. After the download is completed, an icon appears in the notification area with a message that the updates are ready to be installed. When you select the icon or the message, you can install the new updates in a few steps. For more information about the Automatic Updates feature, see Description of the Automatic Updates feature in Windows.

Download Windows updates

Administrators can download updates from the **Microsoft Download Center** or the **Windows Update Catalog** to deploy to multiple computers. If you want to obtain updates to install later on one or more than one computer, use either the following web sites.

- Windows Update Catalog

  For more information about how to download updates from the Windows Update Catalog, see How to download updates that include drivers and hotfixes from the Windows Update Catalog.

- Microsoft Download Center

  For more information about how to download files from the Microsoft Download Center, see How to obtain Microsoft support files from online services.

Install multiple Windows updates or hotfixes with only one restart

Administrators and IT professionals can install multiple Windows updates or hotfixes with only one restart.

References

For more information about security tools and checklists, see Microsoft Security Response Center.

How to schedule automatic updates in Windows

Article • 09/23/2021 • 4 minutes to read

This article explains how to use the Automatic Updates feature in Windows Server 2003, in Windows XP, and in Windows 2000.

Applies to: Windows 10 – all editions, Windows Server 2012 R2
Original KB number: 327838

Summary

If you're logged on as an administrator, the Automatic Updates feature in Windows notifies you when critical updates are available for your computer. There's a new Automatic Updates feature that you can use to specify the schedule that Windows follows to install updates on your computer. This article describes how to install this new Automatic Updates feature in Windows XP and in Windows 2000 and how to use it to schedule automatic updates.

> **Note**
>
> This new Automatic Updates feature is included with Windows Server 2003.

For additional information about how to configure other Automatic Updates settings in Windows XP, click the following article number to view the article in the Microsoft Knowledge Base:

306525 How to configure and use Automatic Updates in Windows XP

Update the Automatic Updates feature (Windows XP and Windows 2000 only)

> **Note**
>
> If you use Automatic Updates, the feature may have been automatically updated on your computer. To make sure that the new feature is installed, use the procedure that is described in the **Schedule Automatic Updates** section of this article to

confirm that the **Automatically download the updates, and install them on the schedule that I specify** option is available on your computer.

To use the new Automatic Updates feature, install the following updates:

Windows XP Service Pack 1 (SP1). For additional information about how to obtain SP1, click the following article number to view the article in the Microsoft Knowledge Base: 322389 How to obtain the latest Windows XP service pack

> ⓘ **Note**
>
> You must restart your computer after you install this update. Automatic Updates does not download any updates until you have configured it to do so. If Automatic Updates is not configured in 24 hours after you install it, either the network administrator or the user who is logged on locally as an administrator is prompted to configure it.

Schedule automatic updates

> ⓘ **Note**
>
> To modify Automatic Updates settings, you must be logged on as an administrator or a member of the Administrators group. If your computer is connected to a network, network policy settings may prevent you from completing this procedure.

In Windows Server 2003 and in Windows XP

To configure a schedule for Automatic Updates:

1. Click **Start**, click **Control Panel**, and then double-click **System**.
2. On the **Automatic Updates** tab, click **Automatically download the updates, and install them on the schedule that I specify**.
3. Click to select the day and time that you want to download and install updates.

When critical updates are detected, Automatic Updates automatically downloads these updates in the background while you're connected to the Internet. After the download is complete, Automatic Updates waits until the scheduled day and time to install the updates. On the scheduled day and time, all local users receive the following message that has a five-minute countdown timer:

Windows is ready to begin installing the updates available for your computer.

Do you want Windows to install the updates now?

(Windows will restarts your computer if no action is taken within 5:00 minutes)

If you're logged on as an administrator, when you receive this message, you can either click **Yes** to install the updates or click **No** to have Automatic Updates install the updates at the next scheduled day and time. If you don't take any action in five minutes, Windows automatically installs the updates.

> ⓘ **Important**
>
> You may have to restart your computer to complete the update installation.

In Windows 2000

1. Click **Start**, click **Control Panel**, and then double-click **Automatic Updates**.
2. Click **Automatically download the updates, and install them on the schedule that I specify.**
3. Click to select the day and time that you want to download and install updates.

When critical updates are detected, Automatic Updates automatically downloads these updates in the background while you're connected to the Internet. After the download is complete, Automatic Updates waits until the scheduled day and time to install the updates. On the scheduled day and time, all local users receive the following message that has a five-minute countdown timer:

Windows is ready to begin installing the updates available for your computer.

Do you want Windows to install the updates now?

(Windows will restart your computer if no action is taken within 5:00 minutes)

If you're logged on as an administrator, when you receive this message, you can either click **Yes** to install the updates or click **No** to have Automatic Updates install the updates at the next scheduled day and time. If you don't take any action in five minutes, Windows automatically installs the updates.

> ⓘ **Important**
>
> You may have to restart your computer to complete the update installation.

References

For additional information about how to use Automatic Updates, view the following articles:

- Description of the Automatic Updates feature in Windows
- How to configure Automatic Updates by using Group Policy or registry settings

For more information about Software Update Services, visit the following Microsoft Web site:
What's new in Windows 10 deployment

How to address disk space issues that are caused by a large Windows component store (WinSxS) directory

Article • 09/23/2021 • 4 minutes to read

This article provides a resolution to solve the disk space issues that are caused by a large Windows component store (WinSxS) directory.

Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
Original KB number: 2795190

Symptoms

When you examine the size of the C:\Windows folder, you may notice that the C:\Windows\winsxs directory seems to use lots of disk spaces.

Cause

The Windows component store (C:\Windows\winsxs) directory is used during servicing operations within Windows installations. Servicing operations include, but are not limited to, Windows Update, service pack, and hotfix installations.

The component store contains all the files that are required for a Windows installation. And, any updates to those files are also held within the component store as the updates are installed. This causes the component store to grow over time as more updates, features, or roles are added to the installation. The component store uses NTFS hard links between itself and other Windows directories to increase the robustness of the Windows platform.

The component store will show a large directory size because of how the Windows Explorer shell accounts for hard links. The Windows shell will count each reference to a hard link as a single instance of the file for each directory in which the file resides. For example, if a file that is named advapi32.dll is 700 KB and is contained in the component store and in the \Windows\system32 directory, Windows Explorer would inaccurately report that the file consumes 1,400 KB of hard disk space.

Resolution

The component store cannot reside on a volume other than the system volume because of the NTFS hard links. If you try to move the component store, this will result in the inability to correctly install Windows updates, service packs, roles, or features. Additionally, we do not recommend that you manually remove or delete files from the component store.

To reduce the size of the component store directory on a Windows installation, you can decide to make the service pack installation permanent and reclaim used space from the service pack files. However, if you make the service pack installation permanent, the service pack is not removable.

To remove the service pack files from a Windows installation, use the following in-box utilities:

- Windows Server 2008 Service Pack 2 installed: Compcln.exe
- Windows 7 Service Pack 1 or Windows Server 2008 R2 Service Pack 1 installed: DISM /online /Cleanup-Image /SpSuperseded or Disk Cleanup Wizard (cleanmgr.exe)

Scavenging may also be performed proactively on Windows Server 2008 installations by forcing a removal event on the system. Scavenging will try to remove any unwanted system binaries from the installation and enable Windows to reclaim the disk space. To issue an uninstall event on a Windows installation, add and remove any unwanted system component that is not already installed, and then restart the Windows installation. Scavenging will be performed during the following restart of the operating system.

> ⓘ **Note**
>
> Scavenging is performed automatically on Windows 7 and Windows Server 2008 R2 installations.

More information

To reclaim additional disk space on your system, follow these steps:

1. Select **Start**, and then in the **Search Programs and Files** text box, type *Disk cleanup*.
2. Click the **Disk Cleanup** icon, and run the Disk Cleanup tool to determine what files you can delete, based on your configuration.

Additional ways to conserve space on the system volume include the following:

- Move the paging file to another volume on the system.
- Disable hibernation on the system.
- Use the dedicated dump file option to capture memory dump files on another volume on the system.
- Offload user profile and program file directories to another volume on the system.
- Disable system restore points on client installations.
- Clean out all temporary directories and folders by using the Disk Cleanup Wizard (cleanmgr.exe).
- Uninstall unused applications or utilities from the installation.

For more information about the WinSxS folder, see:

- Disk Space
- General guidance on disk provisioning for WinSXS growth

For more information about the system requirements for disks, see:

- Install Windows Server 2008 and Windows Server 2008 R2
- Windows 7 system requirements

Note

- When a product is installed by using Windows Installer, a smaller version of the original .msi data file is stored in the Windows Installer Cache (%windir%\Installer) folder. Over time, this folder may grow larger. Every additional update installation for the installed products such as hotfixes, cumulative updates, or service pack setups also store their relevant .msp or .msi file in the Windows Installer cache. Over time, this folder may grow larger. We do not support and do not recommend that you delete any files in this folder or replace them with files from another computer. Any update to the application relies on the information that is available in the files that are stored in this folder. Without this information, the updates cannot perform their installations correctly.

- The *%windir%\softwaredistribution\downloads* folder is used by Windows Update to store downloaded updates. Typically, you do not have to manage this folder because it is managed by Windows. The typical size of this folder is determined by several factors such as the operating system version, what updates are available at the time, and so on. Therefore, it is difficult to provide

a typical size expectation. If this folder uses lots of disk space, first install all available updates for the system, and then restart the computer. To troubleshoot this issue if the size still remains large, follow these steps:

1. At an elevated command prompt, run the `Net Stop WUAUSERV` command.
2. Delete the contents of the *%windir%\softwaredistribution\downloads* folder.
3. At an elevated command prompt, run the `Net Start WUAUSERV` command:

Updates fix in-place upgrade to Windows 10 problem

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to a problem where an in-place upgrade for Windows 10 on a system that's running Microsoft System Center Configuration Manager hangs.

Applies to: Windows 10 - all editions
Original KB number: 4020149

Symptoms

When you run an in-place upgrade for Windows 10 version 1607 on a system that's running Microsoft System Center Configuration Manager, the upgrade hangs. This problem occurs while the Upgrade Operating System task is running.

Details:

- No errors are logged in the Configuration Manager or the Windows Setup log files.
- The SMSTS.log and Setupact.log files stop logging entries.
- An indicator that a computer is encountering this problem is that Windows Setup hangs during driver inventory. This issue is identified by the following signature in the setupact.log file under `C:\$WINDOWS.~BT\Sources\Panther`:

  > date time CONX Windows::Compat::Appraiser::WicaDeviceInventory::GetInventory (324): Starting Device Inventory.
  > date time CONX Windows::Compat::Appraiser::DriverInventory::GetInventory (204): Starting Driver Inventory.

Resolution

To fix this issue, install the update 4013420.

Package installation of compatibility updates differs from installation of other Windows updates. To install the compatibility update, follow these steps:

1. Download the hotfix from the Microsoft Update Catalog website to a new folder on your Windows desktop.

2. After you download the .cab file, extract its contents to a new folder.
3. Determine the source directory of your Windows 10 version 1607 installation files. You can find this in the properties of your Upgrade Operating System Package.
4. After you determine the source directory, copy the contents of the extracted .cab files into the Source folder of the Windows 10 version 1607 installation files. Click **Yes** to overwrite any existing files.
5. Update the Distribution Points for the Upgrade Operating System Package.
6. Retry the deployments and see whether the issue is corrected.

How to install Service Packs and Hotfixes when Windows is running in Safe mode

Article • 09/23/2021 • 2 minutes to read

This article describes how to best install and remove service packs and hotfix updates on Windows-based computers that are running in Safe mode.

Applies to: Windows 10 - all editions
Original KB number: 818460

Summary

Typically, the installation of service packs and hotfix updates is done when Windows is running normally. You can start your Windows-based computer in Safe mode to help you diagnose problems. Microsoft has the following recommendations for the installation of service packs and hotfixes when your computer doesn't function in normal mode:

Installing Service Packs and Hotfixes

Microsoft recommends that you don't install Windows service packs or hotfix updates when Windows is running in Safe mode.

When you install a service pack or hotfix, the Setup program determines which devices are installed in the computer and which Windows components are enabled. Because certain drivers and components are unavailable when Windows runs in Safe mode, the service pack or update Setup program may incorrectly calculate the components that require updating. If you install a service pack or update while Windows runs in Safe mode, and then you restart Windows normally, you may experience intermittent file errors or registry errors. Additionally, when you try to install a service pack or hotfix update while Windows is running in Safe mode, you may receive an error message similar to the following example:

> ERROR_INSTALL_SERVICE_FAILURE
> 1601 The Windows Installer service could not be accessed.
> Contact your support personnel to verify that the Windows
> Installer service is properly registered.

Because of it, Microsoft recommends that you don't install service packs or updates when Windows is running in Safe mode unless you can't start Windows normally.

> **ⓘ Important**
>
> If you do install a service pack or update while Windows is running in Safe mode, immediately reinstall it after you start Windows normally.

Removing Service Packs and Hotfixes

Microsoft recommends that you don't remove Windows service packs or hotfix updates when Windows is running in Safe mode.

Because the removal (uninstall) program for a service pack or hotfix update only restores settings (file replacements and registry changes) that it previously changed, and because the removal program maintains a record of these changes, no problems are expected to occur when you remove a service pack or hotfix when Windows is running in Safe mode. However, Microsoft recommends that you remove a service pack or hotfix while Windows is running in normal mode, where possible.

Package Manager can install only the first package when you extract two or more packages to the same folder in Windows Vista

Article • 09/23/2021 • 3 minutes to read

This article describes a problem that occurs because Package Manager can't manage two or more packages in the same sandbox.

Applies to: Windows 10 – all editions, Windows Server 2012 R2
Original KB number: 932224

Symptoms

In Windows Vista, the Package Manager tool can install only the first package when you extract two or more packages to the same folder.

For example, consider the following scenario:

- On a computer that is running Windows Vista, you create a C:\Temp folder.
- You download the following hotfix packages to this folder:
  - Windows6.0-KB929761-x86.msu
  - Windows6.0-KB932590-x86.msu

    These hotfix packages are for hotfix 929761 and hotfix 932590.
- You run the following commands to expand the hotfix packages:

  Console

  ```
  c:\temp>expand c:\temp\Windows6.0-KB929761-x86.msu -F:Windows6.0-
  KB929761-x86.cab c:\temp

  c:\temp>expand c:\temp\Windows6.0-KB932590-x86.msu -F:Windows6.0-
  KB932590-x86.cab c:\temp
  ```

- You run the following commands to install the packages:

  Console

```
start /w Pkgmgr /ip /m:c:\temp\Windows6.0-KB929761-x86.cab

start /w Pkgmgr /ip /m:c:\temp\Windows6.0-KB932590-x86.cab
```

In this scenario, Package Manager installs only the package for hotfix 929761.

When this problem occurs, information that resembles the following may appear in the Cbs.log file:

In this example Cbs.log file, Package Manager indicates that it will install the .cab file for hotfix 932590. However, it actually installs the Package_1_for_KB929761~31bf3856ad364e35~x86~~6.0.1.1 package. This is the hotfix 929761 package.

> **Note**
>
> This problem also applies to Windows Server 2008.

Cause

This problem occurs because Package Manager can't manage two or more packages in the same sandbox.

Resolution

To work around this problem perform one of the following methods.

Method 1:

Expand each package to different folder before you installing them with pkgmgr. To do this, type the following commands at a command prompt:

Console

```
Delete update*.*

Mkdir c:\temp\sandbox1

Mkdir c:\temp\sandbox2

Start /w pkgmgr /ip /m:c:\temp\ CabFile /s:c:\temp\sandbox1

Start /w pkgmgr /ip /m:c:\temp\ CabFile /s:c:\temp\sandbox2
```

In these commands, **CabFile** represents the .cab file for the hotfix package.

Method 2:

Another workaround is to use DISM to service Windows Vista SP1 and Windows Server 2008 offline images.

Considerations of using DISM with Windows Server 2008/Vista SP1 Images:

- The Windows image that you're updating must be Windows Vista with SP1 or Windows Server 2008 or later.
- If you're servicing a Windows Vista with SP1 or Windows Server 2008 image, DISM will translate the DISM command to the equivalent Package Manager command so that the image can be updated. DISM provides functional parity to Package Manager.
- Only offline scenarios are supported
- DISM is pre-installed with Windows 7 and Windows Server 2008 R2, and is included in the Windows Automated Installation Kit for Windows 7. The Windows Automated Installation Kit can be installed on Windows Vista and Windows 2008.

Editor note: download link for Win7 waik: The Windows Automated Installation Kit (AIK) for Windows 7

Add the Packages to an Offline Image by Using DISM

1. At an elevated command prompt, navigate to the OPK servicing folder, and type the following command to retrieve the name or index number for the image you want to modify.

   Console

   ```
   Dism /Get-WIMInfo /WimFile:C:\test\images\install.wim
   ```

   > **Note**
   >
   > An index or name value is required for most operations that specify a Windows imaging (WIM) file.

2. Type the following command to mount the offline Windows image.

   Console

   ```
   Dism /Mount-WIM /WimFile:C:\test\images\install.wim /Name:"Windows 7
   HomeBasic" /MountDir:C:\test\offline
   ```

3. At a command prompt, type the following command to add a specific package to the image. You can add multiple packages on one command line. The packages will be installed in the order listed in the command line.

```
Console

Dism /Image:C:\test\offline /Add-Package
/PackagePath:C:\packages\package1.cab
/PackagePath:C:\packages\package2.cab
```

> **Note**
>
> .cab is extracted from .msu file.

4. At a command prompt, type the following command to commit the changes and unmount the image.

```
Console

Dism /Unmount-WIM /MountDir:C:\test\offline /Commit
```

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the "Applies to" section.

Previously released Windows updates are reoffered for some systems

Article • 03/24/2022 • 3 minutes to read

This article lists the previously released updates that will be reoffered for systems and provides a solution to this issue.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 3037986

Symptoms

When systems that were built by using media that contains update rollup 3000850 (the November 2014 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2) rerun Windows Update, the following previously released updates will be reoffered.

Article number	Description
2977765	MS14-053: Description of the security update for the .NET Framework 4.5.1 and the .NET Framework 4.5.2 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: September 9, 2014
2978041	MS14-057: Description of the security update for the .NET Framework 4.5.1 and the .NET Framework 4.5.2 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: October 14, 2014
2978126	MS14-072: Description of the security update for the .NET Framework 4.5.1 and 4.5.2 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: November 11, 2014
2979576	MS14-057: Description of the security update for the .NET Framework 4.5.1 and the .NET Framework 4.5.2 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: October 14, 2014
2894856	Description of the security update for the .NET Framework 4.5.1 on Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: December 10, 2013
3002885	MS14-079: Vulnerabilities in kernel-mode driver could allow denial of service: November 11, 2014
2899189	Update adds support for many camera-specific file formats in Windows 8.1 or Windows RT 8.1: December 2013

Article number	Description
2976536	November 2014 anti-malware platform update for Windows Defender in Windows 8.1 and Windows 8
2990967	Some versions of the OneDrive desktop app for Windows do not update automatically
2998174	Active camera is switched unexpectedly when you review photos in Camera app in Windows 8.1 or Windows Server 2012 R2

Cause

The updates that are listed here were not included in the stand-alone November 2014 update package or released in conjunction with that update package.

Resolution

When you build your reference image, you should either install these updates through Windows Update or download and install them manually.

More information

There are scenarios in which update 2919355 (Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update: April 2014) or will also be reoffered. These scenarios and their resolutions are as follows.

Scenario 1

Images were built by using the April 2014 volume license media, and you have update 3000850 installed.

Resolution Integrate update 2959977 and update 2934018 by using the DISM method. (This method is described later.)

Scenario 2

Images that were built by using the November 2014 or April 2014 volume license media on which one of the following language packs was later installed: cs-cz, da-dk, de-de, el-

gr, es-es, fi-fi, fr-fr, hu-hu, it-it, ja-jp, ko-kr, nb-no, nl-nl, pl-pl, pt-br ,pt-pt, ru-ru, sv-se, tr-tr, zh-cn, zh-hk, zh-tw.

Resolution Install the language packs that are required for the environment before you install update 2913955. Or, install update 2934018 by using the stand-alone installer.

Scenario 3

Images that were built by using the November 2014 volume license media in which a language pack was later installed may be reoffered.

Resolution: Use Windows Update to complete the installation of the missing language components

The DISM method

To integrate packages into an image by using the DISM method, follow these steps:

1. Download the standalone package for the update or updates that you want to integrate.
2. Create a new directory to expand the update package.
3. Extract the update package by using the following command:

   expand -f:* < **path to .msu** > < **destination** >

   For example, the following command expands update 2959977 to the C:\Cabs folder:

   expand -f:* Windows8.1-KB2959977-x64.msu c:\cabs

4. Integrate the expanded cabinet (.cab) file into the image from the expanded package by using the following command:

   DISM /Online /Add-Package /PackagePath:< **path to extracted .cab file from step 3** >

   For example, the command to integrate the update 2959977 .cab file would be as follows:

   DISM /Online /Add-Package /PackagePath:c:\cabs\Windows8.1-KB2959977-x64.cab

Missing Windows Installer cache requires a computer rebuild

Article • 09/23/2021 • 3 minutes to read

This article discusses how to restore missing Windows Installer cache files.

Applies to: Windows 10 - all editions, Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2667628

Summary

The Windows Installer Cache is used to store important files for applications that are installed by using Windows Installer. By default, this cache is located in the c:\windows\installer folder, and it should not be deleted. If the installer cache is compromised, you may not immediately see problems until you take an action such as uninstalling, repairing, or updating a product.

When a product is installed by using the Windows Installer, important files are stored in the Windows Installer cache that are required for uninstalling and updating applications. Missing files cannot be copied between computers because the files are unique.

More information

If application files are missing from the Windows Installer Cache, ask the vendor or support team for the application about the missing files. You must follow the procedures or steps recommended by the application vendor to restore the files. In some cases, you may have to rebuild the operating system and reinstall the application to fix the problem.

Windows support engineers cannot help you recover missing application files from the Windows Installer cache.

If the missing installer cache files are SQL Server files, see How to restore the missing Windows Installer cache files and resolve problems that occur during a SQL Server update.

If the missing installer cache files are Microsoft Office or SharePoint files, follow the instructions in the following topics on the Microsoft website:

- Collect data about Office installations by using Robust Office Inventory Scan
- Utility for Office patch maintenance tasks "log, repair, apply, remove, clean"

Third-party recovery tools

Some third-party entities claim to be able to rebuild or repair the Windows Installer cache. For legal and supportability reasons, we cannot recommend or endorse any of these entities. If you use such third-party products and recommendations, you do this at your own risk. If you have backups for your system that were made before the file deletions, consider the following options:

- System Restore points (available only on client operating systems)
- Restoreable system state backup
- Failure recovery methods that can restore the full system state backup
- Reinstallation of the operating system and all applications

To restore the missing files, a full system state restoration is required. It is not possible to replace only the missing files from a previous backup.

Other error messages

Other error messages might be triggered by missing Windows Installer Cache files. Many of the following messages are SQL-specific and are not limited to this issue. These entries are logged in either the Setup or MSI Verbose log.

- **1612**: The installation source for this product is not available. Verify that the source exists and that you can access it.
- **1620**: This installation package could not be opened. Contact the application vendor to verify that this is a valid Windows Installer package.
- **1635**: Unable to install Windows Installer MSP file
- This update package could not be opened. Verify that the update package exists and that you can access it, or contact the application vendor to verify that this is a valid Windows Installer update package.

  1636: Unable to install Windows Installer MSP file
- **1642**: The upgrade cannot be installed by the Windows Installer service because the program to be upgraded may be missing, or the upgrade may update a

different version of the program. Verify that the program to be upgraded exists on your computer and that you have the correct upgrade.

- **1706**: The endpoint format is invalid.
- **1714**: The older version of Microsoft SQL Server Native Client cannot be removed.

Report availability

We strongly encourage you to download this package from the portal instead of reusing a portable copy. If you submit the results, the latest diagnostic rules will be used. This package is frequently updated.

The report is available immediately after you run this tool without submitting the results to Microsoft. The report is an XML file. It will be located in the user profile Temp folder in a path that resembles the following:

`C:\Users\<UserName>\AppData\Local\Temp\WICFIX_MAIN_Report.xml`

SFC detects Opencl.dll as corrupted in Windows 10

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue that causes SFC to detect Opencl.dll as corrupted in Windows 10.

Applies to: Windows 10, version 1809
Original KB number: 3178332

Symptoms

After you run the `SFC /scannow` command in Windows 10, it detects a corrupted system file. The cbs.log file shows that %windir%\syswow64\opencl.dll is detected to be corrupted.

For more information about how to analyze the `SFC /scannow` result, see Analyze the log file entries that SFC.exe generates in Windows Vista.

Resolution

To fix this issue, run the following command:

```
Console

Dism /online /cleanup-image /restorehealth
```

System File Checker (SFC) incorrectly flags Windows Defender PowerShell module files as corrupted

Article • 12/01/2022 • 2 minutes to read

This article describes an issue where System File Checker incorrectly flags Windows Defender PowerShell module files as corrupted.

Applies to: Windows Client
Original KB number: 4513240

Symptoms

The System File Checker (SFC) tool flags files that are located in the *%windir%\System32\WindowsPowerShell\v1.0\Modules\Defender* folder as corrupted or damaged. When this issue occurs, you see error entries that resemble the following:

> Hashes for file member do not match.

Cause

This is a known issue in Windows 10, version 1607 and later versions, and Windows Defender version 4.18.1906.3 and later versions up to version 4.8.1908.

The files for the Windows Defender PowerShell module that are located in *%windir%\System32\WindowsPowerShell\v1.0\Modules\Defender* ship as part of the Windows image. These files are catalog-signed. However, the manageability component of Windows Defender has a new out-of-band (OOB) update channel. This channel replaces the original files with updated versions that are signed by using a Microsoft certificate that the Windows operating system trusts. Because of this change, SFC flags the updated files as "Hashes for file member do not match."

Future releases of Windows will use the updated files in the Windows image. After this change is implemented, SFC will no longer flag the files.

Resolution

This issue is fixed in the version 4.8.1908 update of Windows Defender. After this update is applied, PowerShell files that are part of the Windows image are not changed, and the SFC tool no longer flags these files. Internet-connected computers that subscribe to the Windows Update channel automatically download and install this update.

To repair the Windows image files on computers that have been affected by this issue, use the DISM tool. To do this, open a Command Prompt window on the affected computer, and run the following commands:

Console

```
dism /online /cleanup-image /restorehealth
sfc /scannow
```

If these commands fail and generate an error message that resembles "File not found," make sure that the Install.wim file is accessible, and then run the following commands:

Console

```
DISM /Online /Cleanup-Image /RestoreHealth /Source:WIM:c:\install.wim:1
/LimitAccess
sfc /scannow
```

For more information about repair commands, see Repair a Windows image.

Description of the standard terminology that is used to describe Microsoft software updates

Article • 09/23/2021 • 3 minutes to read

This article describes the standard terminology that defines the software updates for the Windows Update and Microsoft Update services.

Applies to: Windows 10 - all editions
Original KB number: 824684

Critical update

A widely released fix for a specific problem that addresses a critical, non-security-related bug.

Definition update

A widely released and frequent software update that contains additions to a product's definition database. Definition databases are often used to detect objects that have specific attributes, such as malicious code, phishing websites, or junk mail.

Driver

Software that controls the input and output of a device.

Feature pack

New product functionality that is first distributed outside the context of a product release and that is typically included in the next full product release.

Security update

A widely released fix for a product-specific, security-related vulnerability. Security vulnerabilities are rated by their severity. The severity rating is indicated in the Microsoft security bulletin as critical, important, moderate, or low.

Additional information

Microsoft security updates are available for customers to download and are accompanied by two documents: a security bulletin and a Microsoft Knowledge Base article.

Service pack

A tested, cumulative set of all hotfixes, security updates, critical updates, and updates. Additionally, service packs may contain additional fixes for problems that are found internally since the release of the product. Service packs may also contain a limited number of customer-requested design changes or features.

Tool

A utility or feature that helps complete a task or set of tasks.

Update

A widely released fix for a specific problem. An update addresses a noncritical, non-security-related bug.

Update rollup

A tested, cumulative set of hotfixes, security updates, critical updates, and updates that are packaged together for easy deployment. A rollup generally targets a specific area, such as:

- Security
- A component of a product, such as Internet Information Services (IIS).

Security-only update

An update that collects all the new security updates for a given month and for a given product, addressing security-related vulnerabilities. It's distributed through Windows Server Update Services (WSUS), System Center Configuration Manager and Microsoft Update Catalog. Security vulnerabilities are rated by their severity. The severity rating is indicated in the Microsoft security bulletin as critical, important, moderate, or low. This

Security-only update would be displayed under the title Security Only Quality Update when you download or install the update. It will be classified as an *Important* update.

Monthly Rollup

A tested, cumulative set of updates. They include both security and reliability updates that are packaged together and distributed over the following channels for easy deployment:

- Windows Update
- WSUS
- System Center Configuration Manager
- Microsoft Update Catalog

The Monthly Rollup is product-specific and addresses both new security issues and nonsecurity issues in a single update. It will proactively include updates that were released in the past. Security vulnerabilities are rated by their severity. The severity rating is indicated in the Microsoft security bulletin as critical, important, moderate, or low. This Monthly Rollup would be displayed under the title Security Monthly Quality Rollup when you download or install. This Monthly Rollup will be classified as an *Important* update on Windows Update. It will automatically download and install if your Windows Update settings are configured to automatically download and install Important updates.

Preview of Monthly Rollup

A tested, cumulative set of new updates that are packaged together and distributed over:

- Windows Update
- WSUS
- System Center Configuration Manager
- Microsoft Update Catalog

It's distributed ahead of the release of the next Monthly Rollup for customers to proactively download, test, and provide feedback.

The Preview of Monthly Rollup is product-specific and addresses new non-security updates, and includes fixes from the latest Monthly Rollup. This Preview of Monthly Rollup would be displayed under the title Preview of Monthly Quality Rollup when you download or install. It will be classified as an "Optional" update.

Servicing Stack Updates (SSU)

The servicing stack is the code that installs other operating system updates. Additionally, it contains the component-based servicing stack (CBS), which is a key underlying component for several elements of Windows deployment, such as:

- DISM
- SFC
- Changing Windows features or roles
- Repairing components

The CBS is a small component that typically doesn't have updates released every month.

For more information, see Servicing stack updates.

Switches that you can use with xcopy and xcopy32 commands

Article • 03/24/2022 • 2 minutes to read

This article describes switches that you can use with `xcopy` and `xcopy32` commands.

Applies to: Windows 10 - all editions
Original KB number: 289483

Summary

The `xcopy` and `xcopy32` commands have the same switches. This article describes the switches that are available when you run the commands:

- outside of Windows (in MS-DOS mode).
- from an MS-DOS window.

Syntax and switches in MS-DOS mode

The following command line includes the syntax and the switches that you can use with the `xcopy` and `xcopy32` commands in MS-DOS mode:

```
xcopy **source** [**destination**] [/a | /m] [/d: **date**] [/p] [/s] [/e] [/v] [/w]
```

> **Note**
>
> The square brackets ([]) indicate optional switches. The brackets aren't part of the command.

The following table describes the optional switches you can use with `xcopy` and `xcopy32`:

Optional switches	Description
source	Specifies the file to copy.
destination	Specifies the location and the name of new files.

Optional switches	Description
/a	Copies files with the archive attribute set. This switch doesn't change the attribute.
/m	Copies files with the archive attribute set, and turns off the archive attribute.
/d: date	Copies files changed on or after the specified date.
/p	Prompts you before creating each destination file.
/s	Copies folders and subfolders except empty ones.
/e	Copies any subfolder, even if it's empty.
/v	Verifies each new file.
/w	Prompts you to press a key before copying.

> ⚠ **Warning**
>
> Long file names aren't retained in MS-DOS mode.

> ⓘ **Note**
>
> In Windows Millennium Edition (Me) only, an `/h` switch is added to the `xcopy` and the `xcopy32` commands. This switch copies hidden and system files in MS-DOS mode. However, the `Xcopy` files aren't automatically included on the Windows Me boot disk.

Syntax and switches in MS-DOS window

The following command line includes the syntax and the switches for the `xcopy` and `xcopy32` commands when you run it from an MS-DOS window:

```
xcopy **source** [ **destination** ] [/a | /m] [/d: **date**] [/p] [/s] [/e] [/w] [/c] [/i] [/q] [/f] [/l] [/h] [/r] [/t] [/u] [/k] [/n]
```

> ⓘ **Note**
>
> The square brackets ([]) indicate optional switches. The brackets aren't part of the command.

The following table describes the optional switches you can use with `xcopy` and `xcopy32` when you run the command in an MS-DOS window:

Optional switches	Description
source	Specifies the file to copy.
destination	Specifies the location and the name of new files.
/a	Copies files with the archive attribute set. This switch doesn't change the attribute.
/m	Copies files with the archive attribute set, and turns off the archive attribute.
/d: date	Copies files changed on or after the specified date.
/p	Prompts you before each destination file is created.
/s	Copies folders and subfolders except for empty ones.
/e	Copies any subfolder, even if it's empty.
/w	Prompts you to press a key before copying.
/c	Continues copying even if errors occur.
/i	If the destination doesn't exist, and you're copying more than one file, this switch assumes that the destination is a folder.
/q	Doesn't display file names while copying.
/f	Displays full source and destination file names while copying.
/l	Displays files that are going to be copied.
/h	Copies hidden and system files.
/r	Overwrites read-only files.
/t	Creates a folder structure, but doesn't copy files. Doesn't include empty folders or subfolders. Use the /t with the /e switch to include empty folders and subfolders.
/u	Updates the files that already exist in that destination.
/k	Copies attributes. Typical `xcopy` commands reset read-only attributes.
/y	Overwrites existing files without prompting you.
/-y	Prompts you before overwriting existing files.
/n	Copies using the generated short names.

Sysprep fails after you remove or update Microsoft Store apps that include built-in Windows images

Article • 10/15/2021 • 5 minutes to read

This article discusses an issue that occurs when you remove or update a provisioned Microsoft Store app by using the Microsoft Store and then running sysprep on the computer.

Applies to: Windows 10 - all editions, Windows 11
Original KB number: 2769827

Introduction

Sysprep is a tool for IT administrators who want to prepare an installation of Windows for duplication, auditing, and customer delivery. The guidance in this article is intended for use by support agents and IT professionals. If you are a home user who is encountering issues while using Microsoft Store apps, see Fix problems with apps from Microsoft Store.

Several Microsoft Store apps are built in Windows images. These apps include the Mail, Maps, Messaging, Bing, Travel, and News apps, among others. These apps are known as *provisioned* apps. Provisioned apps are staged in the image and are scheduled to be installed for every user of the Windows image at first logon. In addition to the built-in apps, you can side-load your own line-of-business Microsoft Store apps into the Windows image without having to publish them to the Microsoft Store. You can side-load `Appx` packages by using online or offline servicing commands that are available in DISM.exe or through the DISM PowerShell module.

Symptoms

Consider the following scenarios:

Scenario 1

- You are creating a custom Windows 10 or Windows 11 reference computer that you want to sysprep and capture.
- You want to remove some of the provisioned Microsoft Store apps (`Appx` packages) from this reference computer.

- You run `dism -online /Remove-ProvisionedAppxPackage /PackageName:<packagename>` to deprovision the `Appx` packages.

When you run sysprep operation in this scenario, the operation may fail with the following error:

> System Preparation Tool 3.14
> A fatal error occurred while trying to sysprep the machine

Scenario 2

- You have an existing Windows image, and several Microsoft Store apps are side-loaded in the image.
- You want to remove some of the side-loaded `Appx` packages from your image and customize it further.
- You boot into the reference computer and run one of the following PowerShell commands to remove the provisioning of the `Appx` package:
  - `Remove-AppxProvisionedPackage -PackageName <packagename>`
  - `Remove-ProvisionedAppxPackage -PackageName <packagename>`

When you run sysprep operation in this scenario, the operation may fail with the following error:

> System Preparation Tool 3.14
> A fatal error occurred while trying to sysprep the machine

Scenario 3

- You are creating a Windows 10 or Windows 11 reference image.
- You connect to the Microsoft Store, and then you update the built-in Microsoft Store apps by using the Microsoft Store.

When you run sysprep operation in this scenario, the operation may fail with the following error:

> System Preparation tool 3.14 A fatal error occurred while trying to sysprep the machine

Additionally, in the SetupErr.log, you may notice the following error entries:

> <Date> <Time>, Error SYSPRP Package <PackageFullName> was installed for a user, but not provisioned for all users. This package will not function properly in the

> sysprep image.
> <Date> <Time>, Error SYSPRP Failed to remove apps for the current user: 0x80073cf2.
> <Date> <Time>, Error SYSPRP Exit code of RemoveAllApps thread was 0x3cf2.
> <Date> <Time>, Error [0x0f0082] SYSPRP ActionPlatform::LaunchModule: Failure occurred while executing 'SysprepGeneralize' from C:\Windows\System32\AppxSysprep.dll; dwRet = 0x3cf2
> <Date> <Time>, Error SYSPRP ActionPlatform::ExecuteAction: Error in executing action; dwRet = 0x3cf2
> <Date> <Time>, Error SYSPRP ActionPlatform::ExecuteActionList: Error in execute actions; dwRet = 0x3cf2
> <Date> <Time>, Error SYSPRP SysprepSession::Execute: Error in executing actions from C:\Windows\System32\Sysprep\ActionFiles\Generalize.xml; dwRet = 0x3cf2
> <Date> <Time>, Error SYSPRP RunPlatformActions:Failed while executing SysprepSession actions; dwRet = 0x3cf2
> <Date> <Time>, Error [0x0f0070] SYSPRP RunExternalDlls:An error occurred while running registry sysprep DLLs, halting sysprep execution. dwRet = 0x3cf2
> <Date> <Time>, Error [0x0f00a8] SYSPRP WinMain:Hit failure while processing sysprep generalize internal providers; hr = 0x80073cf2

Cause

Sysprep has an additional provider that's added in Windows to clean `Appx` packages and to generalize the image. The provider works only if the `Appx` package is a per-user package or an all-user provisioned package.

- *Per-user package* means that the `Appx` package is installed for a particular user account and is not available for other users of the computer.
- *All-user package* means that the `Appx` has been provisioned into the image so that all users who use this image can access the app.

If an all-user package that's provisioned into the image was manually deprovisioned from the image but not removed for a particular user, the provider will encounter an error while cleaning out this package during sysprep. The provider will also fail if an all-user package that's provisioned into the image was updated by one of the users on this reference computer.

Resolution

To resolve this issue, remove the package for the user who's running sysprep, and also remove the provisioning. To do this, follow these steps.

> ⓘ **Note**
>
> To prevent Microsoft Store from updating apps, unplug the Internet connection or disable Automatic Updates in Audit mode before you create the image.

1. Run the Import-Module Appx PowerShell cmdlet.
2. Run Import-Module Dism.
3. Run `Get-AppxPackage -AllUsers | Where PublisherId -eq 8wekyb3d8bbwe | Format-List -Property PackageFullName,PackageUserInformation`.

   > ⓘ **Note**
   >
   > - In the output of this last cmdlet, check the users for whom the package is showing up as Installed. Delete these user accounts from the reference computer, or log on to the computer by using these user accounts. Then, run the cmdlet in step 4 to remove the `Appx` package.
   > - This command lists all packages that were published by Microsoft and installed by any user of that reference computer. Because the computer is to be sysprepped, we assume that these user profiles no longer require the package.
   > - If you have manually provisioned apps that belong to other publishers, run the following command to list them:
   >   Get-AppxPackage -AllUsers | Format-List -Property PackageFullName,PackageUserInformation

4. Run `Remove-AppxPackage -Package \<packagefullname>`.
5. Remove the provisioning by running the following cmdlet:

   Remove-AppxProvisionedPackage -Online -PackageName <packagefullname>

If you try to recover from an update issue, you can reprovision the app after you follow these steps.

> ⓘ **Note**

The issue does not occur if you are servicing an offline image. In that scenario, the provisioning is automatically cleared for all users. This includes the user who runs the command.

More information

For more information about how to add and remove apps, see:

- Sideload Apps with DISM
- Add or Remove Packages Offline Using DISM

System Error 126 when you start the Windows Modules Installer service (TrustedInstaller): The specific module could not be found

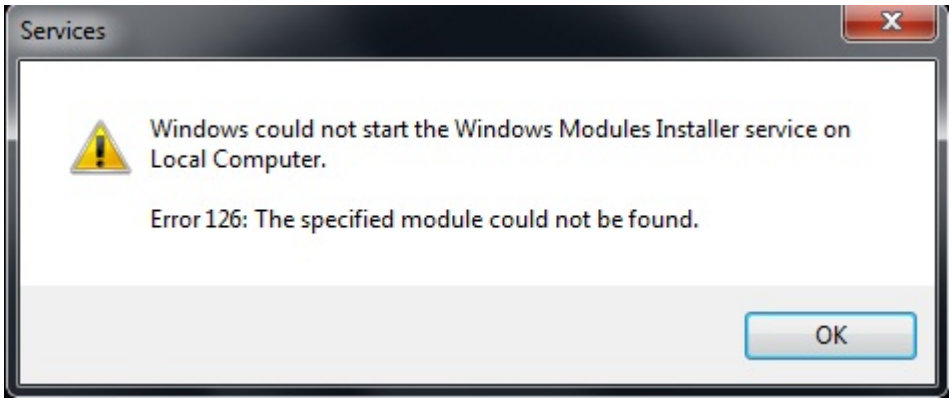
Article • 12/06/2021 • 2 minutes to read

This article helps fix the System Error 126 that occurs when you start the Windows Modules Installer service.

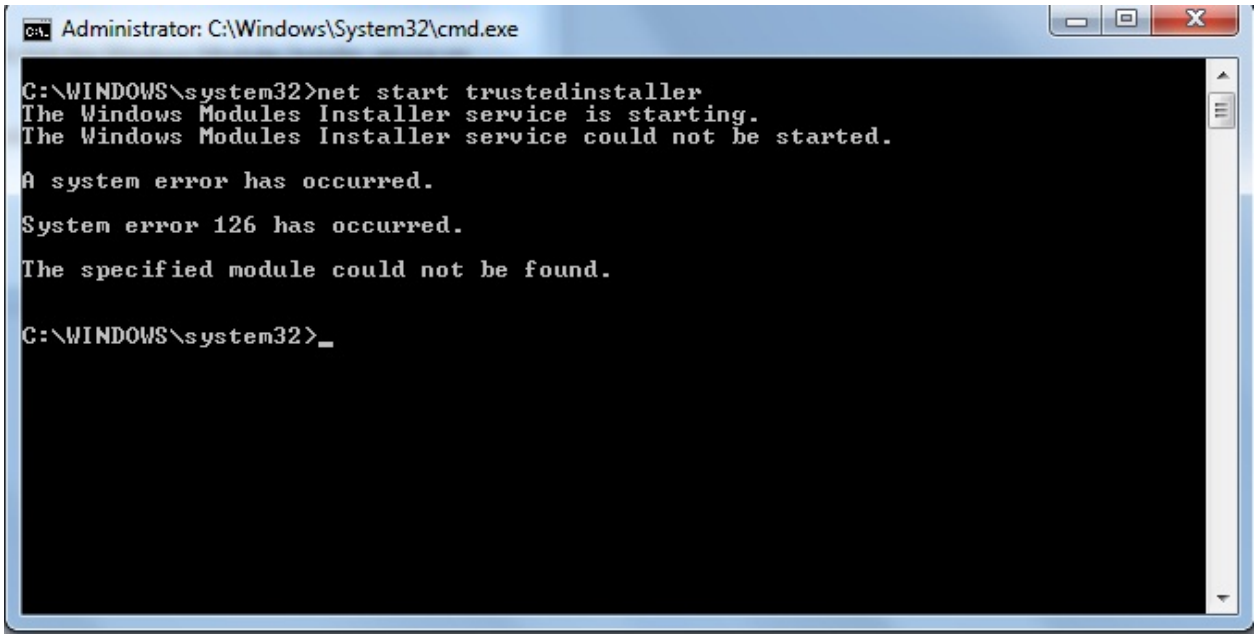
Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
Original KB number: 959077

Symptoms

When you start the Windows Modules Installer service, you receive the following error message:



You also receive an error message at the command prompt:



Cause

This issue occurs if the following registry subkey is changed:

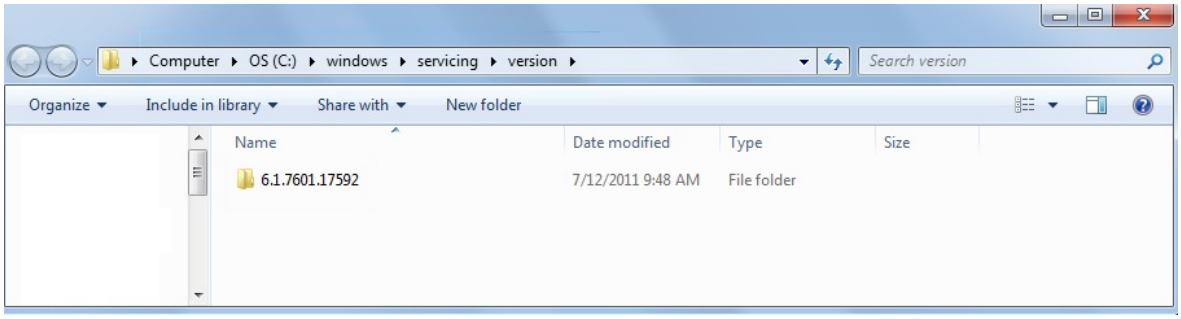
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Version`

Resolution

To resolve this issue, you have to re-create the expandable string value of the registry subkey that is mentioned in the Cause section.

First, you have to check whether the registry subkey exists. To do this, start Registry Editor, and then browse to the subkey that is mentioned in the Cause section. If the subkey does not exist, you must create it. To do this, follow these steps:

1. Locate the `C:\Windows\Servicing\Version` directory, and note the name of the subfolder in this directory. It will be named something like *6.1.7600.16385*. This is your TrustedInstaller ID.
2. Copy the subfolder name to the clipboard, and then paste it into Notepad for safekeeping.



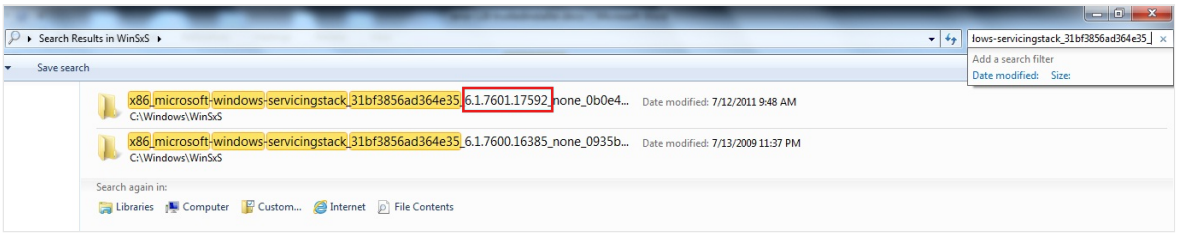
> ⓘ **Note**
>
> In this example, the TrustedInstaller ID is 6.1.7601.17592.

3. In the `C:\Windows\WinSxS` directory, find a subfolder whose name begins with one of the following strings. (In the following subfolder names, the placeholder **TrustedInstaller ID** represents your TrustedInstaller ID.)

   For 32-bit Windows: x86_microsoft-windows-servicingstack_31bf3856ad364e35_ **TrustedInstaller ID** _none

   For 64-bit Windows: amd64_microsoft-windows-servicingstack_31bf3856ad364e35_ **TrustedInstaller ID** _none

4. Copy the subfolder name to the clipboard, and then paste it into Notepad for safekeeping.

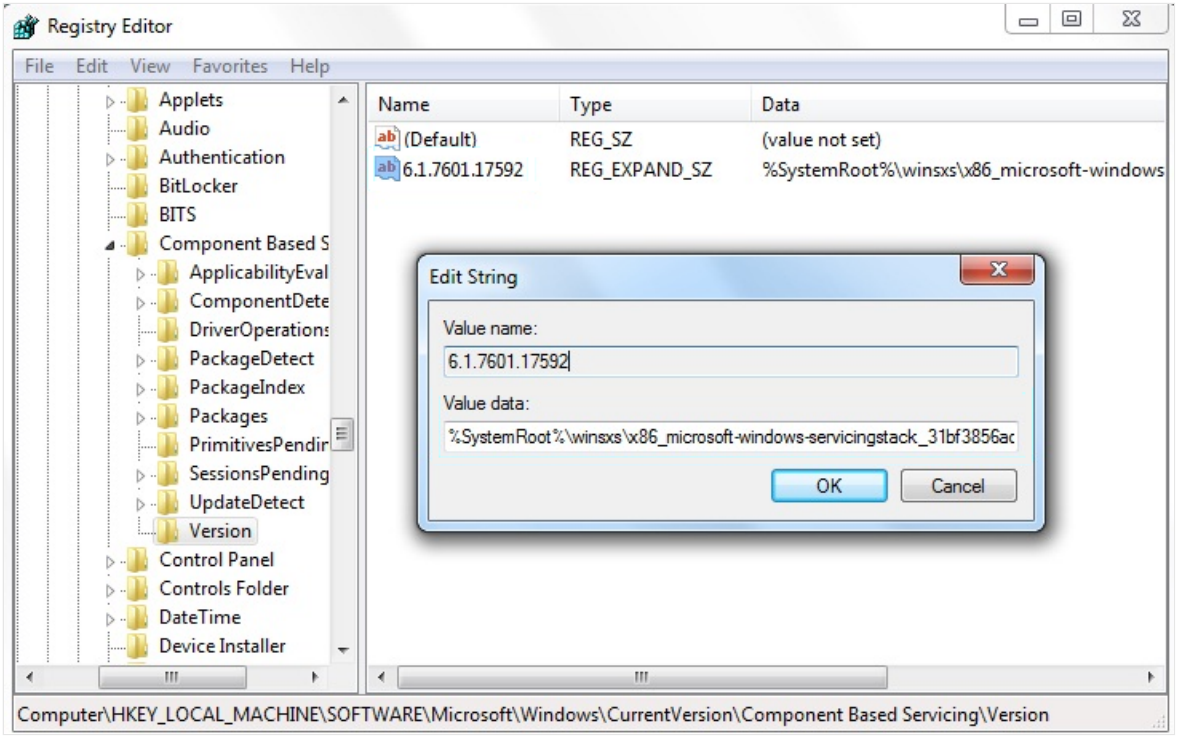


5. Create the registry subkey `HKLM\Software\Microsoft\Windows\CurrentVersion\Component Based Servicing\Version`.

> ⓘ **Note**
>
> To create this key, you have to be an owner of the **Component Based Servicing** key. Then, you have to then give yourself full access permissions.

6. On the **Version** key that you created in step 5, create an expandable string value (or edit it if it already exists). To do this, use the TrustedInstaller ID as your name, and use the full path of the folder that you identified in step 3 as the value.

> **Note**
>
> In the full path, you must use `%SystemRoot%\WinSxS\folder_name` instead of `C:\Windows\WinSxS\folder_name`.



7. Click **OK**, and then exit Registry Editor.

You can now start the Windows Modules Installer (TrustedInstaller) service as usual.

The system registry is no longer backed up to the RegBack folder starting in Windows 10 version 1803

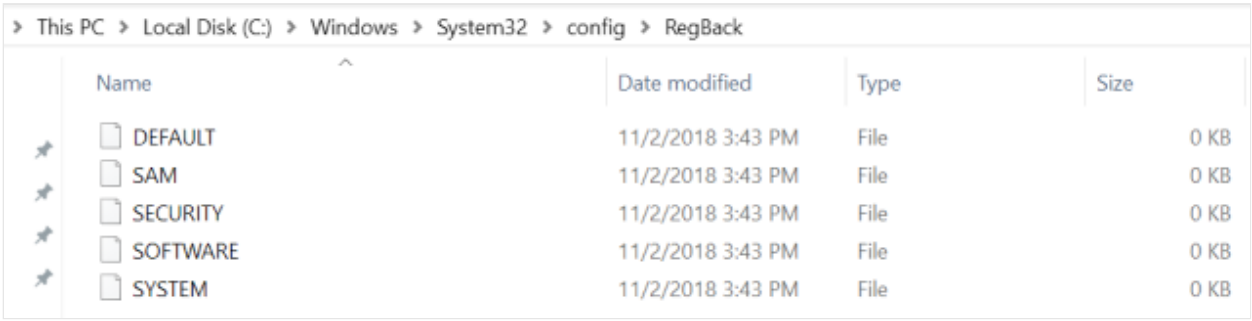
Article • 12/06/2021 • 2 minutes to read

This article discusses a by-design behavior where Windows no longer automatically backs up the system registry to the RegBack folder starting in Windows 10, version 1803.

Applies to: Windows 10 - all editions
Original KB number: 4509719

Summary

Starting in Windows 10, version 1803, Windows no longer automatically backs up the system registry to the RegBack folder. If you browse to the \Windows\System32\config\RegBack folder in Windows Explorer, you will still see each registry hive, but each file is 0 kb in size.



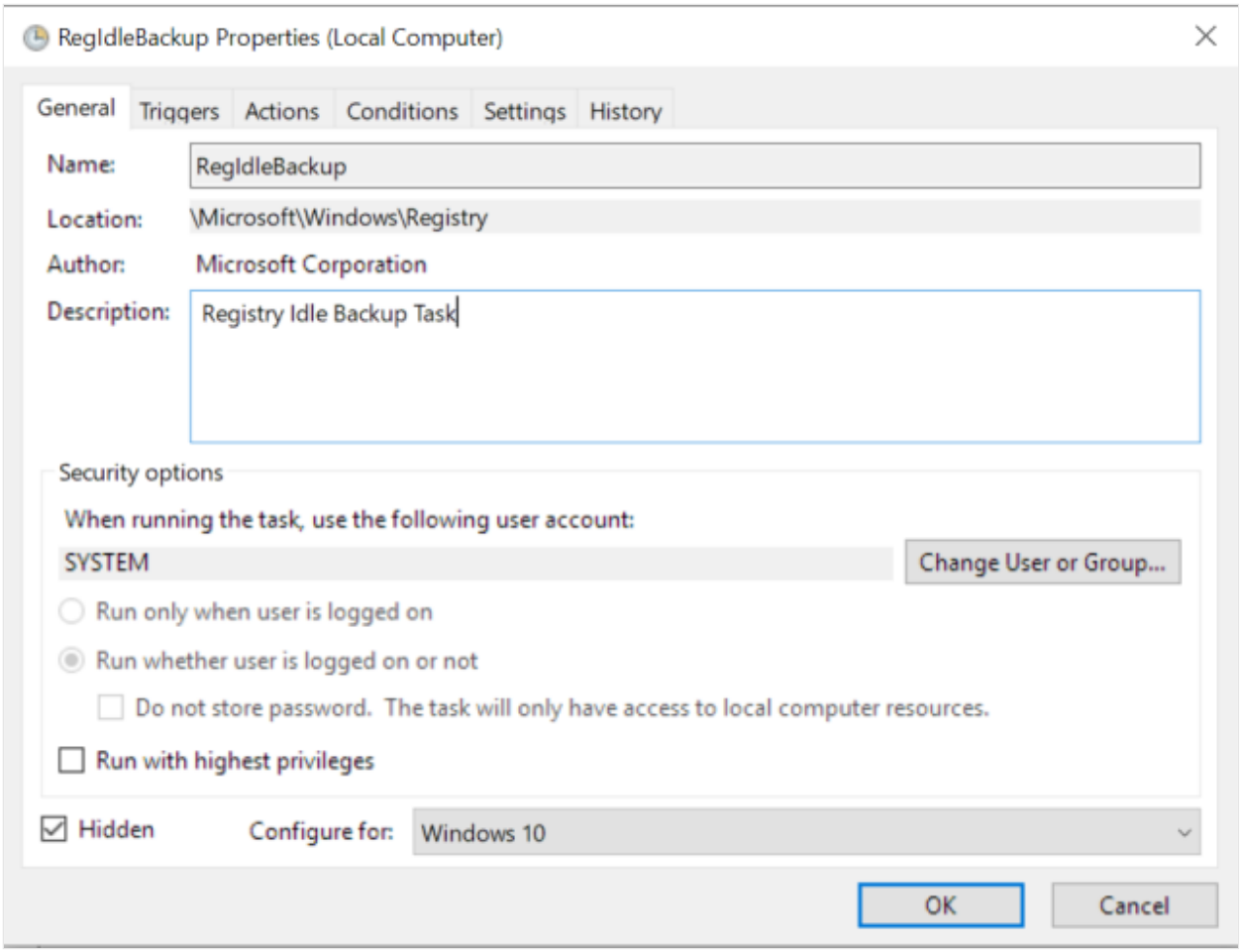
More information

This change is by design, and is intended to help reduce the overall disk footprint size of Windows. To recover a system with a corrupt registry hive, Microsoft recommends that you use a system restore point.

If you have to use the legacy backup behavior, you can re-enable it by configuring the following registry entry, and then restarting the computer:

- Path: `HKLM\System\CurrentControlSet\Control\Session Manager\Configuration Manager\EnablePeriodicBackup`
- Type: REG_DWORD
- Value: 1

Windows backs up the registry to the RegBack folder when the computer restarts, and creates a RegIdleBackup task to manage subsequent backups. Windows stores the task information in the Scheduled Task Library, in the Microsoft\Windows\Registry folder. The task has the following properties:



Windows Update "Processor Not Supported" errors

Article • 12/30/2022 • 2 minutes to read

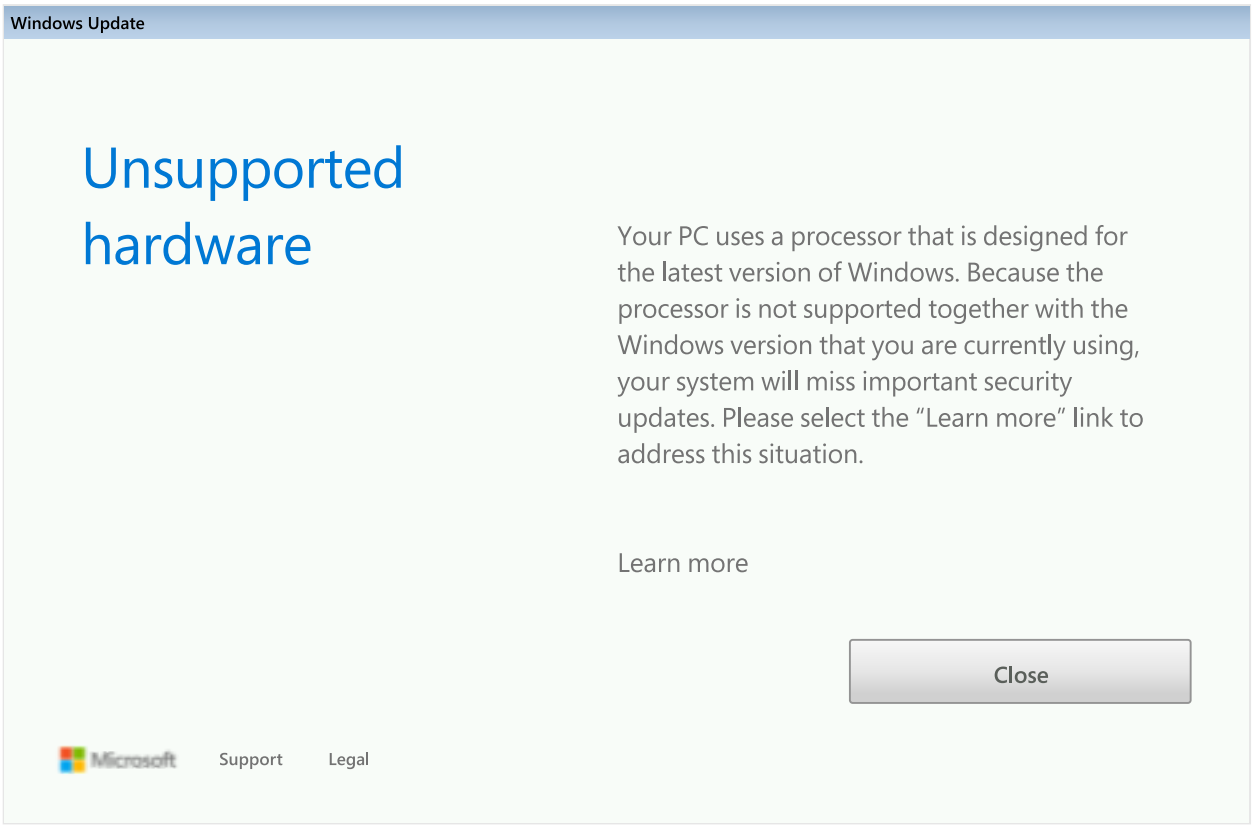
This article discusses the errors "Processor not supported" and "80240037" encountered during Windows Update.

Original KB number: 4012982

Symptoms

When you try to scan or download updates through Windows Update, you receive the following error message:

> Unsupported hardware
> Your PC uses a processor that is designed for the latest version of Windows. Because the processor is not supported together with the Windows version that you are currently using, your system will miss important security updates.



Additionally, you may see the following error message in the Windows Update window:

> Windows could not search for new updates
> An error occurred while checking for new updates for your computer. Error(s) found: Code 80240037 Windows Update encountered an unknown error.

Solution

Since these errors occur when Windows detects an incompatible processor, ensure that Windows is compatible with the processor you're using. Refer to the following documentation for the latest processor generations and models that are supported in different Windows editions:

- For supported Windows Client Processors
- For supported Windows Server Processors
- For supported Windows IoT Core Processors

Additional resources

- Windows Processor Requirements
- Windows Server support and installation instructions for the AMD EPYC 7000 Series server processors
- Lifecycle support policy FAQ -Windows products

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Windows Update or Microsoft Update repeatedly offers the same update

Article • 09/23/2021 • 2 minutes to read

This article describes how to troubleshoot a problem where you are repeatedly offered the same update in Windows Update or Microsoft Update.

Applies to: Windows 10 - all editions, Windows 7 Service Pack 1
Original KB number: 910339

Cause

This may happen if the update isn't installed correctly the first time, or if your Windows Update settings can't detect the update.

Resolution

If you keep seeing the same update being offered for installation, try to install the update later.

You may also want to check your update history to see whether there are any error messages. Then, you can search for any errors that you find by going to the Microsoft Support.

To check your update history, follow these steps.

- For Windows 8

    1. Swipe in from the right side to view the charms, tap or click **Search**, and then type *View Update History*.
    2. Tap or click **Settings**, and then select **View update history**.
    3. Tap or click **Status** to sort by status, and then look for any updates that have a status of **Failed**.
    4. Tap-and-hold or right-click an update that has a status of **Failed**, and then select **View Details**. The window that opens displays the error code for that update.

- For Windows 7, Windows Vista, and Windows XP

    1. Start Windows Update. To do this, click **Start**, type *Update* in the search box, and then, in the list of results, click **Windows Update**.

2. In the navigation pane, click **View update history**.
3. Click **Status** to sort by status, and then look for any updates that have a status of **Failed**.
4. Right-click an update that has a status of **Failed**, and then select **View Details**. The window that opens displays the error code for that update. If this problem persists, post this issue to the Microsoft Communities.

You can also check the telephone number to contact Microsoft Support for help. Charges may apply.

Update the Windows Update Agent to the latest version

Article • 03/24/2022 • 6 minutes to read

This article describes how to update the Windows Update Agent to the latest version.

Applies to: Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012
Original KB number: 949104

Summary

If you have automatic updating turned on, the latest version of the Windows Update Agent is downloaded and installed automatically on your computer. Or, you can manually download and install the Windows Update Agent.

Automatically download Windows Update Agent

To download the Windows Update Agent automatically, follow these steps:

1. Turn on automatic updating. Follow these steps, for the version of Windows that you are running.

    - Windows 8.1 or Windows 8
        a. Open Windows Update by swiping in from the right edge of the screen (or, if you're using a mouse, pointing to the lower-right corner of the screen and moving up the mouse pointer), tapping or clicking **Settings**, tapping or clicking **Control Panel**, and then tapping or clicking **Windows Update**.
        b. Tap or click **Change settings**.
        c. Under **Important updates**, choose **Install updates automatically**.
        d. Under **Recommended updates**, select the **Give me recommended updates the same way I receive important updates** check box, and then select **OK**.

    - Windows 7, Windows Vista, or Windows XP

        To turn on automatic updating automatically, select the **Fix it** button or link, and then select **Run** in the **View Download** dialog box. Then, follow the steps in the **Fix it** wizard.

2. Restart the Windows Update service. To do this, follow these steps:
   a. Press the Windows logo Key+R to open the **Run** box.
   b. Type *services.msc* in the **Run** box, and then press Enter.
   c. Right-click **Windows Update** in the Services management console, and then select **Stop**. If you are running Windows XP, right-click **Automatic Updates**, and then select **Stop**.
   d. After Windows Update stops, right-click **Windows Update**, and then select **Start**. If you are running Windows XP, right-click **Automatic Updates**, and then select **Start**.

3. Wait for Windows Update to start, and then verify that the Windows Update Agent is updated.

Manually download Windows Update Agent from Microsoft Download Center

Click the download link for your version of Windows to obtain the latest Windows Update Agent.

Stand-alone packages for Windows 8 and Windows Server 2012

The following files are available for download from the Microsoft Download Center.

Operating system	Update
All supported x86-based versions of Windows 8 (KB2937636)	Download the package now.
All supported x64-based versions of Windows 8 (KB2937636)	Download the package now.
All supported x64-based versions of Windows Server 2012 (KB2937636)	Download the package now.

Stand-alone packages for Windows 7 SP1 and Windows Server 2008 R2 SP1

The following files are available for download from Windows Update.

Operating system	Update

Operating system	Update
All supported x86-based versions of Windows 7 SP1	Download the package now.
All supported x64-based versions of Windows 7 SP1	Download the package now.
All supported x86-based versions of Windows Server 2008 R2 SP1	Download the package now.
All supported x64-based versions of Windows Server 2008 R2 SP1	Download the package now.
All supported Itanium-based versions of Windows Server 2008 R2 SP1	Download the package now.

> **Note**
>
> Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 with update 2919355 already include the latest version of the Windows Update Agent.

More information

If you receive a Windows Update error, try Solutions for common Windows Update errors.

For more information about how to check which version of the Windows Update Agent is installed, follow these steps:

1. Open the `%systemroot%\system32` folder. `%systemroot%` is the folder in which Windows is installed. For example, the `%systemroot%` folder is `C:\Windows`.
2. Right-click Wuaueng.dll, and then select **Properties**.
3. Select the **Details** tab, and then locate the file version number.

> **Note**
>
> The latest version of the Windows Update Agent for Windows 8.1 is 7.9.9600.16422. The latest version of the Windows Update Agent for Windows 8 is 7.8.9200.16693. The latest version of the Windows Update Agent for Windows 7, Windows Vista, and Windows XP is 7.6.7600.256.

Improvements in version 7.6.7600.256 of Windows Update Agent

- A hardened infrastructure so that the Windows Update client will trust only those files that are signed by a new certificate. The certificate is used solely to protect updates to the Windows Update client.
- A more secure communication channel for the Windows Update client

Improvements in version 7.4.7600.226 of Windows Update Agent

- Improved scan times for Windows updates.
- Improved Windows Update UI for computers that are running Windows Vista or Windows Server 2008.
- More visible and detailed descriptions of updates.
- Improvements in how users are notified about service packs.

Issues that are fixed in version 7.2.6001.788 of Windows Update Agent

Version 7.2.6001.788 of the Windows Update Agent fixes the following issue. This issue was not previously documented in a Microsoft Knowledge Base article:

- When you try to install 80 or more updates at the same time from Windows Update or Microsoft Update, you receive a "0x80070057" error code.

Improvements in version 7.2.6001.784 of Windows Update Agent

- Improved scan times for Windows Update
- Improved speed at which signature updates are delivered
- Support for Windows Installer reinstallation
- Improved error messaging

Issues that are fixed by version 7.0.6000.381 of Windows Update Agent

Version 7.0.6000.381 of the Windows Update Agent fixes the following issues. These issues were not previously documented in a Microsoft Knowledge Base article:

- The Background Intelligent Transfer Service (BITS) crashes on a Windows Vista-based computer. For more information, see An update is available to fix a Background Intelligent Transfer Service (BITS) crash on a Windows Vista-based computer.
- A fix is included that reduces the number of restarts that are required for the stand-alone installer when Multilingual User Interface Pack (MUI) files are being used.
- User interface elements in the Korean, Simplified Chinese, and Traditional Chinese languages are fixed.
- The Windows Vista installation experience is improved.

Windows Update helps keep your computer up-to-date and secure by downloading and installing the latest security and other updates from Microsoft. Windows Update determines which updates apply to your computer.

Microsoft periodically makes software updates available to users of Windows and other Microsoft software. These include updates that improve reliability and performance, updates that provide new protections against malware and other potentially unwanted software, and upgrades to Windows features. To improve the performance or the reliability of hardware components on the computer, Microsoft may also provide updates to device drivers that are supplied by the computer manufacturer.

If you turn on Windows Update, software components that are directly related to Windows Update will have to be updated occasionally on your computer. These updates must be performed before Windows Update can check for required updates or before it can install other updates. These required updates fix errors, provide ongoing improvements, and maintain compatibility with the Microsoft servers that support Windows Update. If you disable Windows Update, you will not receive these updates.

Windows Update is configured to install updates automatically when you select the recommended option during Windows Out Of Box Experience (OOBE) Setup. You can also turn on Windows Update by selecting one of following settings in the Automatic Updates item in Control Panel:

- Automatic (recommended).
- Download updates for me, but let me choose when to install them.
- Notify me, but don't automatically download or install them.

After you turn on Windows Update, the required updates to components of Windows Update will be downloaded and installed automatically without notifying you. This behavior occurs regardless of which setting you use to turn on Windows Update. If you do not want to receive required updates, you can disable automatic updates in Control Panel.

The updates to Windows Update itself typically do the following: Address feedback from customers, improve compatibility, service performance and reliability, and enable new service capabilities. When the Windows Update server is updated, a corresponding client update is typically required. During an agent self-update operation, Windows Update Agent files may be added, modified, or replaced. For example, Windows Update Agent files that help display the user experience or that determine whether updates apply to a particular system may be added. This behavior occurs when a system is set to automatically check for available updates. This does not occur when automatic updates are turned off. For example, this behavior does not occur if you select **Never check for updates** in Windows Vista and Windows 7 or if you select **Turn off Automatic Updates** in Windows XP.

Administrators will receive the latest version of the Windows Update Agent for deployment through Windows Server Update Services (WSUS).

View the system registry by using 64-bit versions of Windows

Article • 09/23/2021 • 2 minutes to read

This article describes how to view the Windows registry by using 64-bit versions of Windows.

Applies to: Windows 10 - all editions
Original KB number: 305097

Summary

The registry in 64-bit versions of Windows is divided into 32-bit and 64-bit keys. Many of the 32-bit keys have the same names as their 64-bit counterparts, and vice versa.

The default 64-bit version of Registry Editor (Regedit.exe) that is included with 64-bit versions of Windows displays both 64-bit keys and 32-bit keys. The WOW64 registry redirector presents 32-bit programs with different keys for 32-bit program registry entries. In the 64-bit version of Registry Editor, 32-bit keys are displayed under the `HKEY_LOCAL_MACHINE\Software\WOW6432Node` registry key.

View 64-bit and 32-bit registry keys

You can view or edit both 64-bit and 32-bit registry keys and values by using the default 64-bit version of Registry Editor. To view or edit 64-bit keys, you must use the 64-bit version of Registry Editor (Regedit.exe). You can also view or edit 32-bit keys and values by using the 32-bit version of Registry Editor in the `%systemroot%\Syswow64` folder. There are no differences in the way you perform tasks between the 32-bit version of Registry Editor and the 64-bit version of Registry Editor. To open the 32-bit version of Registry Editor, follow these steps:

1. Click **Start**, and then click **Run**.
2. In the **Open** box, type `%systemroot%\syswow64\regedit`, and then click **OK**.

> **Note**
>
> You must close the 64-bit version of Registry Editor before you can open the 32-bit version (and vice versa) unless you start the second instance of Registry

> Editor with the `-m` switch. For example, if the 64-bit version of Registry Editor is already running, type `%systemroot%\syswow64\regedit -m` in step 2 to start the 32-bit version of Registry Editor.

To support the co-existence of 32-bit and 64-bit COM registration and program states, WOW64 presents 32-bit programs with an alternate view of the registry. 32-bit programs see a 32-bit `HKEY_LOCAL_MACHINE\Software` tree (`HKEY_LOCAL_MACHINE\Software\WOW6432Node`) that is completely separate from the true 64-bit `HKEY_LOCAL_MACHINE\Software` tree. This isolates `HKEY_CLASSES_ROOT`, because the per-computer portion of this tree resides within the `HKEY_LOCAL_MACHINE\Software` registry key.

To enable 64-bit/32-bit program interoperability through COM and other mechanisms, WOW64 uses a Registry Reflector that mirrors certain registry keys and values between the 64-bit and 32-bit registry views. The reflector is intelligent, in that is only reflects COM activation data.

Reflected keys

The WOW64 Registry reflector may modify the contents of keys and values during the reflection process to adjust path names, and so on. Because of this, the 32-bit and 64-bit contents may differ. For example, pathnames that contain the **system32** registry entry are written as **SysWOW64** in the 32-bit section of the registry. The following keys are reflected:

- `HKEY_LOCAL_MACHINE\Software\Classes`
- `HKEY_LOCAL_MACHINE\Software\COM3`
- `HKEY_LOCAL_MACHINE\Software\Ole`
- `HKEY_LOCAL_MACHINE\Software\EventSystem`
- `HKEY_LOCAL_MACHINE\Software\RPC`

Windows Update automatically downloads and installs updates when you connect to the Internet for the first time

Article • 09/23/2021 • 2 minutes to read

This article describes that if you select the default Windows Update option when you install Windows Vista, important updates are automatically downloaded and installed.

Applies to: Windows Vista
Original KB number: 931275

Summary

In Windows Vista, when you connect to the Internet for the first time, you're prompted to install driver updates, critical software updates, and recommended software updates. Or, if you select the default Windows Update option when you install Windows Vista, these updates are automatically downloaded and installed. So you don't have to wait until the scheduled time to download the updates. By default, updates are downloaded and installed at 3:00 A.M. every morning.

This process occurs regardless of how you connect to the Internet. For example, this process occurs whether you connect to the Internet by using a cable connection, a DSL connection, or a dial-up modem.

More information

We recommend that you use Windows Update to check for the updated hardware drivers.

To manually update Windows Vista by using Windows Update, follow these steps:

1. Select **Start**, type update in the **Start Search** box, and then select **Windows Update** in the **Programs** list.
2. In the upper-left corner of the **Windows Update** window, select **Check for updates**.
3. Select **View available updates** when you're presented with a summary of available updates.

4. In the **View available updates** window, click to select the updates that you want to install, and then select **Install**.

Error on a computer that has a USB device or SD card attached: This PC can't be upgraded to Windows 10

Article • 11/26/2021 • 2 minutes to read

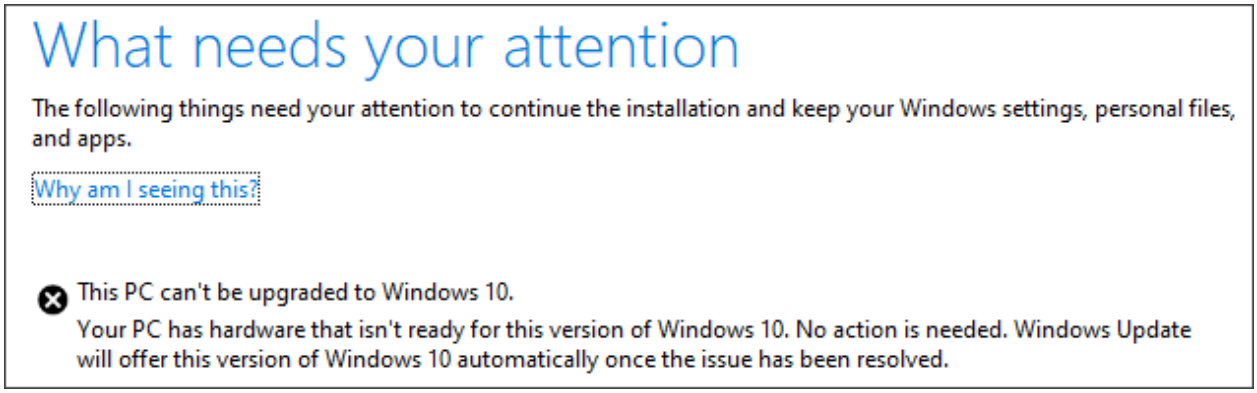
This article helps fix an error that occurs on a computer that has a USB device or SD card attached when you try to upgrade to the May 2019 Feature Update for Windows 10 (Windows 10, version 1903).

Applies to: Windows 10, version 1903
Original KB number: 4500988

Symptoms

If you are trying to upgrade to the May 2019 Feature Update for Windows 10 (Windows 10, version 1903), you may experience an upgrade hold and receive the following message:

> This PC can't be upgraded to Windows 10.



Cause

If you have an external USB device, SD memory card or UFS card attached when installing Windows 10, version 1903, you may get an error message stating "This PC can't be upgraded to Windows 10." This is caused by inappropriate drive reassignment during installation.

An external USB device, SD memory card, or UFS card that is attached to the computer can cause an inappropriate drive reassignment on Windows 10-based computers during

the installation of the Windows 10, version 1903 update. For this reason, there is an update hold on computers to prevent them from receiving Windows 10, version 1903 if this situation is detected. This generates the error message that is mentioned in the Symptoms section if the upgrade is tried again on an affected computer.

Sample scenario

An update to Windows 10, version 1903 is tried on a computer that has a thumb drive inserted into a USB port. Before the update, the thumb drive is mounted in the system as drive G based on the existing drive configuration. However, after the feature update is installed, the device is assigned a different drive letter (for example, drive H).

> **Note**
>
> The drive reassignment is not limited to removable drives. Internal hard drives may also be affected.

To safeguard your update experience, we have applied a hold on devices with an external USB device or SD memory card attached from being offered Windows 10, version 1903 until this issue is resolved.

Workaround

To work around this problem, remove all external media, such as USB devices, SD cards, and UFS cards, from your computer. Then, restart installation of the Windows 10, version 1903 feature update. The update should now proceed normally.

If you are using installation media (USB flash drive, DVD, or ISO file) to install Windows 10, copy the files on the installation media to your local drive, and then start the installation from the local drive.

Status

Microsoft has confirmed that this is a problem in Windows 10, version 1903.

Windows Update hangs and new updates are uninstalled after a restart

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where Windows Update hangs and newly installed updates are uninstalled after a system restart.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 3064434

Symptoms

Consider the following scenario:

- You have a computer that is running Windows.
- You install updates from Windows Update.
- You restart Windows when you are prompted to do this.

In this scenario, you see the following message during the restart process:

> Working on updates
> 13% complete
> Don't turn off your computer

This is an expected message. However, the system appears to stop responding (hangs) for about 15 minutes. After this time, the system does restart. However, the updates that you installed are now uninstalled.

Additionally, an entry that resembles the following may be logged in the CBS.log file under %SystemRoot%\Logs\CBS:

> Shtd: Timed out waiting for shutdown processing to complete - no progress detected in last 900000 milliseconds

Cause

This issue occurs because the Trusted Installer service did not finish the installation process within the default time-out period of 15 minutes.

Workaround

To work around this issue, set the time-out value to a larger value in the registry, and then reapply the hotfix. To do this, follow these steps:

1. Start Registry Editor.
2. Locate the following subkey:
   `HKLM\System\CurrentControlSet\Services\TrustedInstaller`
3. Right-click the **TrustedInstaller** key, and then click **Permissions**.
4. Grant the **Full Control** user right to the Administrators group.
5. Change the **BlockTimeIncrement** value to 2a30 (Hexadecimal).

   > **Note**
   >
   > This change sets the time-out value to three hours. This should be sufficient for most situations. However, you may have to try a larger value in your environment.

6. Restart the server, and then apply the hotfix again.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the "Applies to" section.

Resolution procedures

Article • 10/17/2022 • 19 minutes to read

Applies to: Windows 10

> **Note**
>
> This is a 200 level topic (moderate).
>
> See **Resolve Windows 10 upgrade errors** for a full list of topics in this article.

This article provides some common causes and solutions that are associated with specific upgrade error codes. If a Windows 10 upgrade fails, you can write down the error code that is displayed, or find the error code in the Windows Event Log or in the Windows Setup log files (ex: *setuperr.log*) and review the cause and solutions provided here. You should also try running the free SetupDiag tool provided by Microsoft, which can automatically find the reason for an upgrade failure.

0xC1900101

A frequently observed result code is 0xC1900101. This result code can be thrown at any stage of the upgrade process, with the exception of the downlevel phase. 0xC1900101 is a generic rollback code, and usually indicates that an incompatible driver is present. The incompatible driver can cause blue screens, system hangs, and unexpected reboots. Analysis of supplemental log files is often helpful, such as:

- The minidump file: *$Windows.~bt\Sources\Rollback\setupmem.dmp*
- Event logs: *$Windows.~bt\Sources\Rollback*.evtx*
- The device install log: *$Windows.~bt\Sources\Rollback\setupapi\setupapi.dev.log*

The device install log is helpful if rollback occurs during the sysprep operation (extend code 0x30018).

To resolve a rollback that was caused by driver conflicts, try running setup using a minimal set of drivers and startup programs by performing a clean boot before initiating the upgrade process.

See the following general troubleshooting procedures associated with a result code of 0xC1900101:

Code	Mitigation	Cause
0xC1900101 - 0x20004	Uninstall antivirus applications. Remove all unused SATA devices. Remove all unused devices and drivers. Update drivers and BIOS.	Windows Setup encountered an error during the SAFE_OS with the INSTALL_RECOVERY_ENVIRONMENT operation. This error is caused by out-of-date drivers.
0xC1900101 - 0x2000c	Disconnect all peripheral devices that are connected to the system, except for the mouse, keyboard and display. Contact your hardware vendor to obtain updated device drivers. Ensure that "Download and install updates (recommended)" is accepted at the start of the upgrade process.	Windows Setup encountered an unspecified error during Wim apply in the WinPE phase. This error is caused by out-of-date drivers

Code	Mitigation	Cause
0xC1900101 - 0x20017	Ensure that all that drivers are updated. Open the Setuperr.log and Setupact.log files in the %windir%\Panther directory, and then locate the problem drivers. For more information, see Windows Vista, Windows 7, Windows Server 2008 R2, Windows 8.1, and Windows 10 setup log file locations. Update or uninstall the problem drivers.	A driver has caused an illegal operation. Windows wasn't able to migrate the driver, resulting in a rollback of the operating system. This is a SafeOS boot failure, typically caused by drivers or non-Microsoft disk encryption software. This can also be caused by a hardware failure.
0xC1900101 - 0x30018	Disconnect all peripheral devices that are connected to the system, except for the mouse, keyboard and display. Contact your hardware vendor to obtain updated device drivers. Ensure that "Download and install updates (recommended)" is accepted at the start of the upgrade process.	A device driver has stopped responding to setup.exe during the upgrade process.
0xC1900101 - 0x3000D	Disconnect all peripheral devices that are connected to the system, except for the mouse, keyboard and display. Update or uninstall the display driver.	Installation failed during the FIRST_BOOT phase while attempting the MIGRATE_DATA operation. This can occur due to a problem with a display driver.
0xC1900101 - 0x4000D	Check supplemental rollback logs for a setupmem.dmp file, or event logs for any unexpected reboots or errors. Review the rollback log and determine the stop code. The rollback log is located in the *$Windows.~BT\Sources\Rollback* folder. An example analysis is shown below. This example isn't representative of all cases: Info SP Crash 0x0000007E detected Info SP Module name : Info SP Bugcheck parameter 1: 0xFFFFFFFFC0000005 Info SP Bugcheck parameter 2: 0xFFFFF8015BC0036A Info SP Bugcheck parameter 3: 0xFFFFD000E5D23728 Info SP Bugcheck parameter 4: 0xFFFFD000E5D22F40 Info SP Can't recover the system. Info SP Rollback: Showing splash window with restoring text: Restoring your previous version of Windows. Typically, there's a dump file for the crash to analyze. If you aren't equipped to debug the dump, then attempt the following basic troubleshooting procedures: 1. Make sure you have enough disk space. 2. If a driver is identified in the bug check message, disable the driver or check with the manufacturer for driver updates. 3. Try changing video adapters. 4. Check with your hardware vendor for any BIOS updates. 5. Disable BIOS memory options such as caching or shadowing.	A rollback occurred due to a driver configuration issue. Installation failed during the second boot phase while attempting the MIGRATE_DATA operation. This can occur because of incompatible drivers.

Code	Mitigation	Cause
0xC1900101 - 0x40017	Clean boot into Windows, and then attempt the upgrade to Windows 10. For more information, see How to perform a clean boot in Windows. Ensure that you select the option to "Download and install updates (recommended)." Computers that run Citrix VDA You may see this message after you upgrade a computer from Windows 10, version 1511 to Windows 10, version 1607. After the second system restart, the system generates this error and then rolls back to the previous version. This problem has also been observed in upgrades to Windows 8.1 and Windows 8. This problem occurs because the computer has Citrix Virtual Delivery Agent (VDA) installed. Citrix VDA installs device drivers and a file system filter driver (CtxMcsWbc). This Citrix filter driver prevents the upgrade from writing changes to the disk, so the upgrade can't complete and the system rolls back. Resolution To resolve this problem, install Cumulative update for Windows 10 Version 1607 and Windows Server 2016: November 8, 2016. You can work around this problem in two ways: Workaround 1 1. Use the VDA setup application (VDAWorkstationSetup_7.11) to uninstall Citrix VDA. 2. Run the Windows upgrade again. 3. Reinstall Citrix VDA. Workaround 2 If you can't uninstall Citrix VDA, follow these steps to work around this problem: 1. In Registry Editor, go to the following subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4d36e967-e325-11ce-bfc1-08002be10318}\CtxMcsWbc` 2. Change the value of the `Start` entry from **0** to **4**. This change disables the Citrix MCS cache service. 3. Go to the following subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class{4d36e967-e325-11ce-bfc1-08002be10318}` 4. Delete the `CtxMcsWbc` entry. 5. Restart the computer, and then try the upgrade again. Non-Microsoft information disclaimer The non-Microsoft products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.	Windows 10 upgrade failed after the second reboot. This is caused by a faulty driver. For example: antivirus filter drivers or encryption drivers.

0x800xxxxx

Result codes that start with the digits 0x800 are also important to understand. These error codes indicate general operating system errors, and aren't unique to the Windows upgrade process. Examples include timeouts, devices not functioning, and a process stopping unexpectedly.

See the following general troubleshooting procedures associated with a result code of 0x800xxxxx:

Code	Mitigation	Cause
80040005 - 0x20007	This error has more than one possible cause. Attempt quick fixes, and if not successful, analyze log files in order to determine the problem and solution.	An unspecified error occurred with a driver during the SafeOS phase.
0x80073BC3 - 0x20009 0x80070002 - 0x20009 0x80073B92 - 0x20009	These errors occur during partition analysis and validation, and can be caused by the presence of multiple system partitions. For example, if you installed a new system drive but left the previous system drive connected, this can cause a conflict. To resolve the errors, disconnect or temporarily disable drives that contain the unused system partition. You can reconnect the drive after the upgrade has completed. Alternatively, you can delete the unused system partition.	The requested system device can't be found, there's a sharing violation, or there are multiple devices matching the identification criteria.
800704B8 - 0x3001A	Disable or uninstall non-Microsoft antivirus applications, disconnect all unnecessary devices, and perform a clean boot.	An extended error has occurred during the first boot phase.
8007042B - 0x4000D	Analyze log files in order to determine the file, application, or driver that isn't able to be migrated. Disconnect, update, remove, or replace the device or object.	The installation failed during the second boot phase while attempting the MIGRATE_DATA operation. This issue can occur due to file system, application, or driver issues.
8007001F - 0x3000D	Analyze log files in order to determine the files or registry entries that are blocking data migration. This error can be due to a problem with user profiles. It can occur due to corrupt registry entries under `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList` or invalid files in the *\Users* directory. Note: If a previous upgrade didn't complete, invalid profiles might exist in the *Windows.old\Users* directory. To repair this error, ensure that deleted accounts aren't still present in the Windows registry and that files under the *\Users* directory are valid. Delete the invalid files or user profiles that are causing this error. The specific files and profiles that are causing the error will be recorded in the Windows setup log files.	The installation failed in the FIRST_BOOT phase with an error during MIGRATE_DATA operation.

Code	Mitigation	Cause
8007001F - 0x4000D	Analyze log files in order to determine the device that isn't functioning properly. Disconnect, update, or replace the device.	General failure, a device attached to the system isn't functioning.
8007042B - 0x4001E	This error has more than one possible cause. Attempt quick fixes, and if not successful, analyze log files in order to determine the problem and solution.	The installation failed during the second boot phase while attempting the PRE_OOBE operation.

Other result codes

Error code	Cause	Mitigation
0xC1800118	WSUS has downloaded content that it can't use due to a missing decryption key.	See Steps to resolve error 0xC1800118 for information.
0xC1900200	Setup.exe has detected that the machine doesn't meet the minimum system requirements.	Ensure the system you're trying to upgrade meets the minimum system requirements. See Windows 10 specifications for information.
0x80090011	A device driver error occurred during user data migration.	Contact your hardware vendor and get all the device drivers updated. It's recommended to have an active internet connection during upgrade process. Ensure that "Download and install updates (recommended)" is accepted at the start of the upgrade process.
0xC7700112	Failure to complete writing data to the system drive, possibly due to write access failure on the hard disk.	This issue is resolved in the latest version of Upgrade Assistant. Ensure that "Download and install updates (recommended)" is accepted at the start of the upgrade process.
0x80190001	An unexpected error was encountered while attempting to download files required for upgrade.	To resolve this issue, download and run the media creation tool. See Download windows 10.
0x80246007	The update wasn't downloaded successfully.	Attempt other methods of upgrading the operating system. Download and run the media creation tool. See Download windows 10. Attempt to upgrade using .ISO or USB. Note: Windows 10 Enterprise isn't available in the media creation tool. For more information, go to the Volume Licensing Service Center.

Error code	Cause	Mitigation
0x80244018	Your machine is connected through a proxy server.	Make sure Automatically Detect Settings is selected in internet options. (**Control Panel** > **Internet Options** > **Connections** > **LAN Settings**).
0xC1900201	The system didn't pass the minimum requirements to install the update.	Contact the hardware vendor to get the latest updates.
0x80240017	The upgrade is unavailable for this edition of Windows.	Administrative policies enforced by your organization might be preventing the upgrade. Contact your IT administrator.
0x80070020	The existing process can't access the file because it's being used by another process.	Use the MSCONFIG tool to perform a clean boot on the machine and then try to perform the update again. For more information, see How to perform a clean boot in Windows.
0x80070522	The user doesn't have required privilege or credentials to upgrade.	Ensure that you've signed in as a local administrator or have local administrator privileges.
0xC1900107	A cleanup operation from a previous installation attempt is still pending and a system reboot is required in order to continue the upgrade.	Restart the device and run setup again. If restarting the device doesn't resolve the issue, then use the Disk Cleanup utility to clean up the temporary files and the System files. For more information, see Disk cleanup in Windows 10.
0xC1900209	The user has chosen to cancel because the system doesn't pass the compatibility scan to install the update. Setup.exe will report this error when it can upgrade the machine with user data but cannot migrate installed applications.	Incompatible software is blocking the upgrade process. Uninstall the application and try the upgrade again. For more information, see Windows 10 Pre-Upgrade Validation using SETUP.EXE. You can also download the Windows Assessment and Deployment Kit (ADK) for Windows 10 and install Application Compatibility Tools.
0x8007002	This error is specific to upgrades using Configuration Manager R2 SP1 CU3 (5.00.8238.1403)	Analyze the SMSTS.log and verify that the upgrade is failing on "Apply Operating system" Phase: Error 80072efe DownloadFileWithRanges() failed. 80072efe. ApplyOperatingSystem (0x0760) The error 80072efe means that the connection with the server was terminated abnormally. To resolve this issue, try the OS Deployment test on a client in same VLAN as the Configuration Manager server. Check the network configuration for random client-server connection issues happening on the remote VLAN.

Error code	Cause	Mitigation
0x80240FFF	Occurs when update synchronization fails. It can occur when you're using Windows Server Update Services on its own or when it's integrated with Microsoft Endpoint Configuration Manager. If you enable update synchronization before you install hotfix 3095113, WSUS doesn't recognize the Upgrades classification, and instead treats the upgrade like a regular update.	You can prevent this by installing hotfix 3095113 before you enable update synchronization. However, if you have already run into this problem, do the following steps: 1. Disable the Upgrades classification. 2. Install hotfix 3095113. 3. Delete previously synched updates. 4. Enable the Upgrades classification. 5. Perform a full synch. For detailed information on how to run these steps check out How to delete upgrades in WSUS.
0x8007007E	Occurs when update synchronization fails because you don't have hotfix 3095113 installed before you enable update synchronization. Specifically, the CopyToCache operation fails on clients that have already downloaded the upgrade because Windows Server Update Services has bad metadata related to the upgrade. It can occur when you're using standalone Windows Server Update Services or when WSUS is integrated with Microsoft Endpoint Configuration Manager.	Use the following steps to repair Windows Server Update Services. You must run these steps on each WSUS server that synched metadata before you installed the hotfix. Stop the Windows Update service. • Sign in as a user with administrative privileges, and then do the following steps: • Open **Administrative Tools** from the **Control Panel**. • Double-click **Services**. • Find the **Windows Update** service, right-click it, and then select **Stop**. If prompted, enter your credentials. Delete all files and folders under *c:\Windows\SoftwareDistribution\DataStore*. Restart the Windows Update service.

Other error codes

Error Codes	Cause	Mitigation
0x80070003-0x20007	This is a failure during SafeOS phase driver installation.	Verify device drivers on the computer, and analyze log files to determine the problem driver.
0x8007025D - 0x2000C	This error occurs if the ISO file's metadata is corrupt or if there's an issue with the storage medium, such as a RAM module containing bad blocks during the installation of Windows.	Redownload the ISO/Media and reattempt the upgrade Alternatively, re-create installation media the Media Creation Tool.
0x80070490 - 0x20007	An incompatible device driver is present.	Verify device drivers on the computer, and analyze log files to determine the problem driver.

Error Codes	Cause	Mitigation
0xC1900101 - 0x2000c	An unspecified error occurred in the SafeOS phase during WIM apply. This can be caused by an outdated driver or disk corruption.	Run checkdisk to repair the file system. For more information, see the quick fixes section in this guide. Update drivers on the computer, and select "Download and install updates (recommended)" during the upgrade process. Disconnect devices other than the mouse, keyboard and display.
0xC1900200 - 0x20008	The computer doesn't meet the minimum requirements to download or upgrade to Windows 10.	See Windows 10 Specifications and verify the computer meets minimum requirements. Review logs for compatibility information.
0xC1900200 - 0x20008	The computer doesn't meet the minimum requirements to download or upgrade to Windows 10. See Windows 10 Specifications and verify the computer meets minimum requirements. Review logs for Windows 10 Specifications.	
0x80070004 - 0x3000D	This is a problem with data migration during the first boot phase. There are multiple possible causes.	Analyze log files to determine the issue.
0xC1900101 - 0x4001E	Installation failed in the SECOND_BOOT phase with an error during PRE_OOBE operation.	This is a generic error that occurs during the OOBE phase of setup. See the 0xC1900101 section of this guide and review general troubleshooting procedures described in that section.
0x80070005 - 0x4000D	The installation failed in the SECOND_BOOT phase with an error in during MIGRATE_DATA operation. This error indicates that access was denied while attempting to migrate data.	Analyze log files to determine the data point that is reporting access denied.
0x80070004 - 0x50012	Windows Setup failed to open a file.	Analyze log files to determine the data point that is reporting access problems.

Error Codes	Cause	Mitigation
0xC190020e 0x80070070 - 0x50011 0x80070070 - 0x50012 0x80070070 - 0x60000	These errors indicate the computer doesn't have enough free space available to install the upgrade.	To upgrade a computer to Windows 10, it requires 16 GB of free hard drive space for a 32-bit OS, and 20 GB for a 64-bit OS. If there isn't enough space, attempt to free up drive space before proceeding with the upgrade. **Note:** If your device allows it, you can use an external USB drive for the upgrade process. Windows setup will back up the previous version of Windows to a USB external drive. The external drive must be at least 8 GB (16 GB is recommended). The external drive should be formatted using NTFS. Drives that are formatted in FAT32 may run into errors due to FAT32 file size limitations. USB drives are preferred over SD cards because drivers for SD cards aren't migrated if the device doesn't support Connected Standby.

Modern setup errors

Also see the following sequential list of modern setup (mosetup) error codes with a brief description of the cause.

Result code	Message	Description
0XC1900100	MOSETUP_E_VERSION_MISMATCH	An unexpected version of Setup Platform binaries was encountered. Verify the package contents.
0XC1900101	MOSETUP_E_SETUP_PLATFORM	The Setup Platform has encountered an unspecified error.
0XC1900102	MOSETUP_E_SHUTDOWN_BLOCK	Unable to create or destroy the shutdown block message.
0XC1900103	MOSETUP_E_COMPAT_TIMEOUT	The compatibility issues weren't resolved within the required time limit.
0XC1900104	MOSETUP_E_PROCESS_TIMEOUT	The installation process did not complete within the required time limit.
0XC1900105	MOSETUP_E_TEST_MODE	The installation process is being used in a test environment.
0XC1900106	MOSETUP_E_TERMINATE_PROCESS	The installation process was terminated.
0XC1900107	MOSETUP_E_CLEANUP_PENDING	A cleanup operation from a previous installation attempt is still pending. A system reboot is required.

Result code	Message	Description
0XC1900108	MOSETUP_E_REPORTING	An error has occurred and the result value must be consolidated for telemetry purposes.
0XC1900109	MOSETUP_E_COMPAT_TERMINATE	The installation process was terminated during the actionable compatibility phase.
0XC190010a	MOSETUP_E_UNKNOWN_CMD_LINE	The installation process was launched with an unknown command-line argument.
0XC190010b	MOSETUP_E_INSTALL_IMAGE_NOT_FOUND	The installation image was not found.
0XC190010c	MOSETUP_E_AUTOMATION_INVALID	The provided automation information was invalid.
0XC190010d	MOSETUP_E_INVALID_CMD_LINE	The installation process was launched with an invalid command-line argument.
0XC190010e	MOSETUP_E_EULA_ACCEPT_REQUIRED	The installation process requires that the user accept the license agreement.
0XC1900110	MOSETUP_E_EULA_CANCEL	The user has chosen to cancel for license agreement.
0XC1900111	MOSETUP_E_ADVERTISE_CANCEL	The user has chosen to cancel for advertisement.
0XC1900112	MOSETUP_E_TARGET_DRIVE_NOT_FOUND	Could not find a target drive letter.
0XC1900113	MOSETUP_E_EULA_DECLINED	The user has declined the license terms.
0XC190011e	MOSETUP_E_FLIGHTING_BVT	The installation process has been halted for testing purposes.
0XC190011f	MOSETUP_E_PROCESS_CRASHED	The installation process crashed.
0XC1900120	MOSETUP_E_EULA_TIMEOUT	The user has not accepted the EULA within the required time limit.
0XC1900121	MOSETUP_E_ADVERTISE_TIMEOUT	The user has not accepted Advertisement within the required time limit.
0XC1900122	MOSETUP_E_DOWNLOADDISKSPACE_TIMEOUT	The download disk space issues were not resolved within the required time limit.

Result code	Message	Description
0XC1900123	MOSETUP_E_INSTALLDISKSPACE_TIMEOUT	The install disk space issues were not resolved within the required time limit.
0XC1900124	MOSETUP_E_COMPAT_SYSREQ_TIMEOUT	The minimum requirements compatibility issues were not resolved within the required time limit.
0XC1900125	MOSETUP_E_COMPAT_DOWNLOADREQ_TIMEOUT	The compatibility issues for download were not resolved within the required time limit.
0XC1900126	MOSETUP_E_GATHER_OS_STATE_SIGNATURE	The GatherOsState executable has invalid signature.
0XC1900127	MOSETUP_E_UNINSTALL_ALLOWED_ABORT	The user has chosen to abort Setup to keep Uninstall option active.
0XC1900128	MOSETUP_E_MISSING_TASK	The install cannot continue because a required task is missing.
0XC1900129	MOSETUP_E_UPDATEMEDIA_REQUESTED	A more up-to-date version of setup will be launched to continue installation
0XC190012f	MOSETUP_E_FINALIZE_ALREADY_REQUESTED	The install cannot continue because a finalize operation was already requested.
0XC1900130	MOSETUP_E_INSTALL_HASH_MISSING	The install cannot continue because the instance hash was not found.
0XC1900131	MOSETUP_E_INSTALL_HASH_MISMATCH	The install cannot continue because the instance hash does not match.
0XC19001df	MOSETUP_E_DISK_FULL	The install cannot continue because the system is out of disk space.
0XC19001e0	MOSETUP_E_GATHER_OS_STATE_FAILED	The GatherOsState executable has failed to execute.
0XC19001e1	MOSETUP_E_PROCESS_SUSPENDED	The installation process was suspended.
0XC19001e2	MOSETUP_E_PREINSTALL_SCRIPT_FAILED	A preinstall script failed to execute or returned an error.
0XC19001e3	MOSETUP_E_PRECOMMIT_SCRIPT_FAILED	A precommit script failed to execute or returned an error.
0XC19001e4	MOSETUP_E_FAILURE_SCRIPT_FAILED	A failure script failed to execute or returned an error.

Result code	Message	Description
0XC19001e5	MOSETUP_E_SCRIPT_TIMEOUT	A script exceeded the timeout limit.
0XC1900200	MOSETUP_E_COMPAT_SYSREQ_BLOCK	The system does not pass the minimum requirements to install the update.
0XC1900201	MOSETUP_E_COMPAT_SYSREQ_CANCEL	The user has chosen to cancel because the system does not pass the minimum requirements to install the update.
0XC1900202	MOSETUP_E_COMPAT_DOWNLOADREQ_BLOCK	The system does not pass the minimum requirements to download the update.
0XC1900203	MOSETUP_E_COMPAT_DOWNLOADREQ_CANCEL	The user has chosen to cancel because the system does not pass the minimum requirements to download the update.
0XC1900204	MOSETUP_E_COMPAT_MIGCHOICE_BLOCK	The system does not pass the requirements for desired migration choice.
0XC1900205	MOSETUP_E_COMPAT_MIGCHOICE_CANCEL	The user has chosen to cancel because the system does not pass the requirements for desired migration choice.
0XC1900206	MOSETUP_E_COMPAT_DEVICEREQ_BLOCK	The system does not pass the device scan to install the update.
0XC1900207	MOSETUP_E_COMPAT_DEVICEREQ_CANCEL	The user has chosen to cancel because the system does not pass the device scan to install the update.
0XC1900208	MOSETUP_E_COMPAT_INSTALLREQ_BLOCK	The system does not pass the compat scan to install the update.
0XC1900209	MOSETUP_E_COMPAT_INSTALLREQ_CANCEL	The user has chosen to cancel because the system does not pass the compat scan to install the update.
0XC190020a	MOSETUP_E_COMPAT_RECOVERYREQ_BLOCK	The system does not pass the minimum requirements to recover Windows.

Result code	Message	Description
0XC190020b	MOSETUP_E_COMPAT_RECOVERYREQ_CANCEL	The user has chosen to cancel because the system does not pass the minimum requirements to recover Windows.
0XC190020c	MOSETUP_E_DOWNLOADDISKSPACE_BLOCK	The system does not pass the disk space requirements to download the payload.
0XC190020d	MOSETUP_E_DOWNLOADDISKSPACE_CANCEL	The user has chosen to cancel as the device does not have enough disk space to download.
0XC190020e	MOSETUP_E_INSTALLDISKSPACE_BLOCK	The system does not pass the disk space requirements to install the payload.
0XC190020f	MOSETUP_E_INSTALLDISKSPACE_CANCEL	The user has chosen to cancel as the device does not have enough disk space to install.
0XC1900210	MOSETUP_E_COMPAT_SCANONLY	The user has used the setup.exe command line to do scanonly, not to install the OS.
0XC1900211	MOSETUP_E_DOWNLOAD_UNPACK_DISKSPACE_BLOCK	The system does not pass the disk space requirements to download and unpack media.
0XC1900212	MOSETUP_E_DOWNLOAD_UNPACK_DISKSPACE_MULTIARCH_BLOCK	The system does not pass the disk space requirements to download and unpack multi-architecture media.
0XC1900213	MOSETUP_E_NO_OFFER_FOUND	There was no offer found that matches the required criteria.
0XC1900214	MOSETUP_E_UNSUPPORTED_VERSION	This version of the tool is not supported.
0XC1900215	MOSETUP_E_NO_MATCHING_INSTALL_IMAGE	Could not find an install image for this system.
0XC1900216	MOSETUP_E_ROLLBACK_PENDING	Found pending OS rollback operation.
0XC1900220	MOSETUP_E_COMPAT_REPORT_NOT_DISPLAYED	The compatibility report cannot be displayed due to a missing system component.
0XC1900400	MOSETUP_E_UA_VERSION_MISMATCH	An unexpected version of Update Agent client was encountered.
0XC1900401	MOSETUP_E_UA_NO_PACKAGES_TO_DOWNLOAD	No packages to be downloaded.

Result code	Message	Description
0XC1900402	MOSETUP_E_UA_UPDATE_CANNOT_BE_MERGED	No packages to be downloaded.
0XC1900403	MOSETUP_E_UA_CORRUPT_PAYLOAD_FILES	Payload files were corrupt.
0XC1900404	MOSETUP_E_UA_BOX_NOT_FOUND	The installation executable was not found.
0XC1900405	MOSETUP_E_UA_BOX_CRASHED	The installation process terminated unexpectedly.

More information

- Windows 10 FAQ for IT professionals
- Windows 10 Enterprise system requirements
- Windows 10 Specifications
- Windows 10 IT pro forums
- Fix Windows Update errors by using the DISM or System Update Readiness tool
- Windows 7 to Windows 10 upgrade error (0x800707E7 - 0x3000D))
- Windows 10 upgrade error: User profile suffix mismatch, 0x800707E7 - 0x3000D

Quick fixes

Article • 10/12/2022 • 9 minutes to read

Applies to: Windows 10

> **Note**
>
> This is a 100 level topic (basic).
>
> See **Resolve Windows 10 upgrade errors** for a full list of topics in this article.

The following list of fixes can resolve many Windows upgrade problems. You should try these steps before contacting Microsoft support, or attempting a more advanced analysis of a Windows upgrade failure. Also review information at Windows 10 help.

The Microsoft Virtual Agent provided by Microsoft Support can help you to analyze and correct some Windows upgrade errors. To talk to a person about your issue, start the Virtual Agent (select **Get started**) and enter *Talk to a person* two times.

> **Tip**
>
> You might also wish to try a new tool available from Microsoft that helps to diagnose many Windows upgrade errors. For more information and to download this tool, see **SetupDiag**. The topic is more advanced (300 level) because several advanced options are available for using the tool. However, you can now just download and then double-click the tool to run it. By default when you click Save, the tool is saved in your *Downloads* folder. Double-click the tool in the folder and wait until it finishes running (it might take a few minutes), then double-click the *SetupDiagResults.log* file and open it using Notepad to see the results of the analysis.

List of fixes

Here are the step-by-step instructions:

1. Remove nonessential external hardware, such as docks and USB devices.
2. Check the system drive for errors and attempt repairs.
3. Run the Windows Update troubleshooter.
4. Attempt to restore and repair system files.

5. Update Windows so that all available recommended updates are installed, and ensure the computer is rebooted if it is necessary to complete installation of an update.
6. Temporarily uninstall non-Microsoft antivirus software.
7. Uninstall all nonessential software.
8. Update firmware and drivers.
9. Ensure that "Download and install updates (recommended)" is accepted at the start of the upgrade process.
10. Verify at least 16 GB of free space is available to upgrade a 32-bit OS, or 20 GB for a 64-bit OS.

Remove external hardware

If the computer is portable and it's currently in a docking station, undock the computer.

Unplug nonessential external hardware devices from the computer, such as:

- Headphones
- Joysticks
- Printers
- Plotters
- Projectors
- Scanners
- Speakers
- USB flash drives
- Portable hard drives
- Portable CD/DVD/Blu-ray drives
- Microphones
- Media card readers
- Cameras/Webcams
- Smart phones
- Secondary monitors, keyboards, mice

For more information about disconnecting external devices, see Safely remove hardware in Windows 10

Repair the system drive

The system drive is the drive that contains the system partition. It is usually the C: drive.

To check and repair errors on the system drive:

1. Select **Start**.
2. Type *command*.
3. Right-click **Command Prompt** and then select **Run as administrator**.
4. If you're prompted by UAC, select **Yes**.
5. Type `chkdsk /F` and press Enter.
6. When you're prompted to schedule a check the next time the system restarts, type `Y`.
7. See the following example.

   Console

   ```
   C:\WINDOWS\system32>chkdsk /F
   The type of the file system is NTFS.
   Cannot lock current drive.

   Chkdsk cannot run because the volume is in use by another
   process.  Would you like to schedule this volume to be
   checked the next time the system restarts? (Y/N) Y

   This volume will be checked the next time the system restarts.
   ```

8. Restart the computer. The computer will pause before loading Windows and perform a repair of your hard drive.

Windows Update Troubleshooter

The Windows Update Troubleshooter tool will automatically analyze and fix problems with Windows Update, such as a corrupted download. It will also tell you if there's a pending reboot that is preventing Windows from updating.

Download the tool for Windows 10 .

To run the tool, select the appropriate link above. Your web browser will prompt you to save or open the file. Select **open** and the tool will automatically start. The tool will walk you through analyzing and fixing some common problems.

You can also download the Windows Update Troubleshooter by starting the Microsoft Virtual Agent , typing *update Windows*, selecting the version of Windows you're running, and then answering **Yes** when asked "Do you need help troubleshooting Windows Update?"

If any errors are displayed in the Windows Update Troubleshooter, use the Microsoft Virtual Agent to ask about these errors. The Virtual Agent will perform a search and provide a list of helpful links.

Repair system files

This fix is also described in detail at answers.microsoft.com.

To check and repair system files:

1. Select **Start**.
2. Type *command*.
3. Right-click **Command Prompt** and then select **Run as administrator**.
4. If you're prompted by UAC, select **Yes**.
5. Type `sfc /scannow` and press Enter. See the following example:

```
Console

C:\>sfc /scannow

Beginning system scan.  This process will take some time.

Beginning verification phase of system scan.
Verification 100% complete.

Windows Resource Protection did not find any integrity violations.
```

6. If you're running Windows 8.1 or later, type `DISM.exe /Online /Cleanup-image /Restorehealth` and press Enter (the `DISM` command options aren't available for Windows 7). See the following example:

```
Console

C:\>DISM.exe /Online /Cleanup-image /Restorehealth

Deployment Image Servicing and Management tool
Version: 10.0.16299.15

Image Version: 10.0.16299.309

[==========================100.0%==========================] The
restore operation completed successfully.
The operation completed successfully.
```

> **Note**
>
> It may take several minutes for the command operations to be completed. For more information, see **Repair a Windows Image** and **Use the System File Checker tool**.

Update Windows

You should ensure that all important updates are installed before attempting to upgrade. This includes updates to hardware drivers on your computer.

The Microsoft Virtual Agent can walk you through the process of making sure that Windows is updated.

Start the Virtual Agent and then type *update windows*.

Answer questions that the agent asks, and follow instructions to ensure that Windows is up to date. You can also run the Windows Update Troubleshooter described above.

Select **Start**, select **Power Options**, and then restart the computer.

Uninstall non-Microsoft antivirus software

Use Windows Defender for protection during the upgrade.

Verify compatibility information, and if desired reinstall antivirus applications after the upgrade. If you plan to reinstall the application after upgrading, be sure that you have the installation media and all required activation information before removing the program.

To remove the application, go to **Control Panel** > **Programs** > **Programs and Features** and select the antivirus application, then select **Uninstall**. Choose **Yes** when you're asked to confirm program removal.

For more information, see Windows 7 - How to properly uninstall programs or Repair or remove programs in Windows 10.

Uninstall non-essential software

Outdated applications can cause problems with a Windows upgrade. Removing old or non-essential applications from the computer can therefore help.

If you plan to reinstall the application later, be sure that you have the installation media and all required activation information before removing it.

To remove programs, use the same steps as are provided above for uninstalling non-Microsoft antivirus software, but instead of removing the antivirus application repeat the steps for all your non-essential, unused, or out-of-date software.

Update firmware and drivers

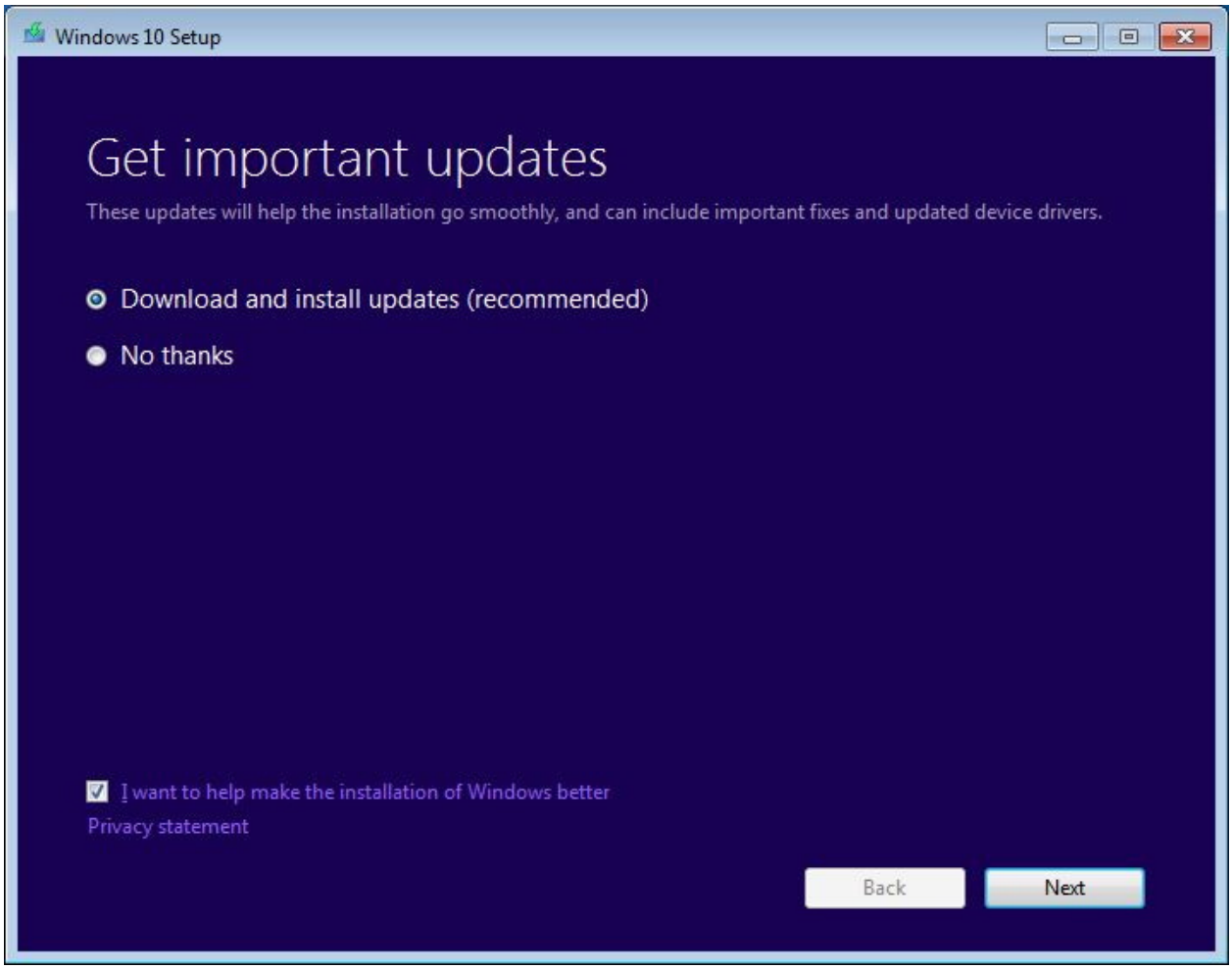
Updating firmware (such as the BIOS) and installing hardware drivers is an advanced task. Don't attempt to update BIOS if you aren't familiar with BIOS settings or aren't sure how to restore the previous BIOS version if there are problems. Most BIOS updates are provided as a "flash" update. Your manufacturer might provide a tool to perform the update, or you might be required to enter the BIOS and update it manually. Be sure to save your working BIOS settings, since some updates can reset your configuration and make the computer fail to boot if (for example) a RAID configuration is changed.

Most BIOS and other hardware updates can be obtained from a website maintained by your computer manufacturer. For example, Microsoft Surface device drivers can be obtained at: Download the latest firmware and drivers for Surface devices.

To obtain the proper firmware drivers, search for the most updated driver version provided by your computer manufacturer. Install these updates and reboot the computer after installation. Request assistance from the manufacturer if you have any questions.

Ensure that "Download and install updates" is selected

When you begin a Windows Update, the setup process will ask you to **Get important updates**. Answer **Yes** if the computer you're updating is connected to the Internet. See the following example:



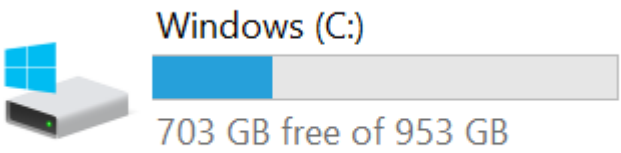
Verify disk space

You can see a list of requirements for Windows 10 at Windows 10 Specifications & System Requirements. One of the requirements is that enough hard drive space be available for the installation to take place. At least 16 GB of free space must be available on the system drive to upgrade a 32-bit OS, or 20 GB for a 64-bit OS.

To view how much hard drive space is available on your computer, open File Explorer. In Windows 7, this was called Windows Explorer.

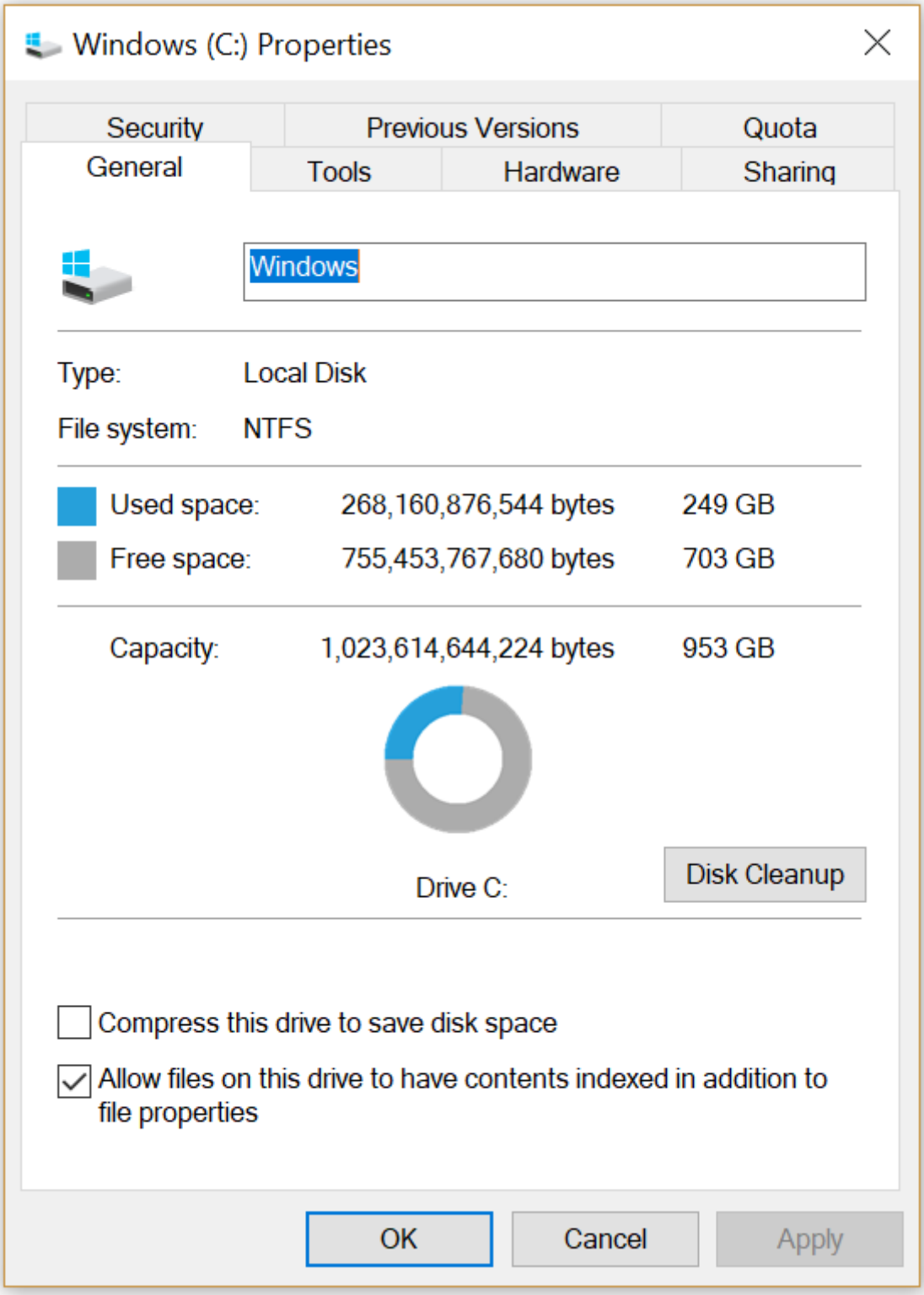
In **File Explorer**, select **Computer** or **This PC** on the left, then look under **Hard Disk Drives** or under **Devices and drives**. If there are multiple drives listed, the system drive is the drive that includes a Microsoft Windows logo above the drive icon.

The amount of space available on the system drive will be displayed under the drive. See the following example:



In the previous example, there's 703 GB of available free space on the system drive (C:).

To free up more space on the system drive, begin by running Disk Cleanup. You can access Disk Cleanup by right-clicking the hard drive icon and then clicking Properties. See the following example:



For instructions to run Disk Cleanup and other suggestions to free up hard drive space, see Tips to free up drive space on your PC.

When you run Disk Cleanup and enable the option to Clean up system files, you can remove previous Windows installations, which can free a large amount of space. You should only do this if you don't plan to restore the old OS version.

Open an elevated command prompt

> **Tip**
>
> It is no longer necessary to open an elevated command prompt to run the **SetupDiag** tool. However, this is still the optimal way to run the tool.

To launch an elevated command prompt, press the Windows key on your keyboard, type *cmd*, press Ctrl+Shift+Enter, and then select **Yes** to confirm the elevation prompt. For more information about screenshots and other steps to open an elevated command prompt, see Command Prompt (Admin) Windows 7.

> **Note**
>
> When you open an elevated command prompt, you will usually start in the *C:\WINDOWS\system32* directory. To run a program that you recently downloaded, you must change to the directory where the program is located. Alternatively, you can move or copy the program to a directory in your PATH variable. These directories are automatically searched. Type `echo %PATH%` to see the directories in your PATH variable.

Another option is to use File Explorer to create a new folder under C: with a short name such as "new" then copy or move the programs you want to run (like SetupDiag) to this folder using File Explorer. When you open an elevated command prompt, change to this directory by typing `cd c:\new`, and now you can run the programs in that folder.

If you downloaded the *SetupDiag.exe* program to your computer, then copied it to the folder *C:\new*, and you opened an elevated command prompt then typed `cd c:\new` to change to this directory, you can just type `setupdiag` and press Enter to run the program. This program will analyze the files on your computer to see why a Windows Upgrade failed and if the reason was a common one, it will report this reason. It will not fix the problem for you but knowing why the upgrade failed enables you to take steps to fix the problem.

More information

- Windows 10 FAQ for IT professionals
- Windows 10 Enterprise system requirements
- Windows 10 Specifications
- Windows 10 IT pro forums
- Fix Windows Update errors by using the DISM or System Update Readiness tool

The .NET Framework 4.5.1 (web installer) for Windows 7 SP1 and Windows Server 2008 R2 SP1

Article • 09/23/2021 • 2 minutes to read

This article provides information about the Microsoft .NET Framework 4.5.1 (web installer) for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1.

Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
Original KB number: 2859818

Introduction

The Microsoft .NET Framework 4.5.1 is a highly compatible, in-place update to the Microsoft .NET Framework 4 and the Microsoft .NET Framework 4.5.

The web installer is a small package (less than 1 megabyte) that automatically determines and downloads only the components applicable for a particular platform. The web installer also installs the language pack that matches the language of the user's operating system.

Download information

The following file is available for download from the Microsoft Download Center:

Download the package now.

For more information about how to download Microsoft support files, see How to obtain Microsoft support files from online services.

Microsoft scanned this file for viruses. Microsoft used the most current virus-detection software that was available on the date that the file was posted. The file is stored on security-enhanced servers that help prevent any unauthorized changes to the file.

What's new in the .NET Framework 4.5.1

The .NET Framework 4.5.1 supports the writing of code in C#, Visual Basic, and F# programming languages, and includes these significant language and framework enhancements:

- Better performance and reliability
- ASP.NET applications suspend and resume
- On-demand compaction of the large object heap
- 64-bit Edit and Continue
- Activity tracing and sampling
- SQL connection resiliency
- Managed return valuesFor more information about these and other features of the .NET Framework 4.5.1, see the .NET Framework Developer Center website. This version of the .NET Framework runs side by side with the Microsoft .NET Framework 3.5 Service Pack 1 (SP1) and earlier versions, but performs an in-place update for the .NET Framework 4 and the .NET Framework 4.5.

Command-line options for this update

For more information about the various command-line options that are supported by this update, go to the Command-Line options section in .NET Framework Deployment Guide for Developers.

Restart requirement

You may have to restart the computer after you install this software if any affected files are being used. We recommend that you close all applications that are using the .NET Framework before you apply this update.

Status

Microsoft has confirmed that this is a problem.

Error when you upgrade to Windows Storage Server 2016 or Windows Server 2016: Windows cannot verify the digital signature for this file

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where an error (Windows cannot verify the digital signature for this file) occurs when you upgrade to Windows Storage Server 2016 or Windows Server 2016.

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2
Original KB number: 3193460

Symptoms

When you try to upgrade the system to Windows Storage Server 2016 or Windows Server 2016, the process fails at 95 percent completion, and you receive the following error message:

> The following errors(s) occurred:
> Windows cannot verify the digital signature for this file. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software form an unknown source An error occurred during automated setup. You must configure your nodes(s) manually.

This issue occurs if the following conditions are true:

- You upgrade Windows Storage Server 2012 R2 to Windows Storage Server 2016 or Windows Server 2012 R2 to Windows Server 2016.
- The original system has the OEM Appliance OOBE feature installed.

Cause

This issue occurs because some OEM systems ship together with a custom out-of-box-experience (OOBE) update. This OOBE update is installed through Deployment Imaging and Management (DISM) and has a special rename operation that replaces the main OOBE feature. This replacement causes the digital signature error.

Workaround

To work around this issue, use DISM to uninstall the OEM Appliance OOBE feature before you upgrade the system. To do this, run the following Dism.exe command:

Console

```
dism /online /disable-feature /featurename:OEM-Appliance-OOBE
```

How to Automate Regional and Language settings in Windows Vista, Windows Server 2008, Windows 7 and in Windows Server 2008 R2

Article • 09/23/2021 • 2 minutes to read

This article describes the regional and language settings options and the method to modify the settings.

Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
Original KB number: 2764405

Summary

This article describes the Regional and Language Settings options in Windows Vista, in Windows Server 2008, in Windows 7 and in Windows Server 2008 R2. Also, in this article you can find the method to modify the settings using an xml based answer file.

Sample XML answer file

XML

```
<gs:GlobalizationServices xmlns:gs="urn:longhornGlobalizationUnattend">

<!-- user list -->
 <gs:UserList>
 <gs:User UserID="Current" CopySettingsToDefaultUserAcct="true"
CopySettingsToSystemAcct="true"/>
 </gs:UserList>

<!-- GeoID -->
 <gs:LocationPreferences>
 <gs:GeoID Value="244"/>
 </gs:LocationPreferences>

<gs:MUILanguagePreferences>
 <gs:MUILanguage Value="cy-GB"/>
 <gs:MUIFallback Value="en-GB"/>
 </gs:MUILanguagePreferences>

<!-- system locale -->
 <gs:SystemLocale Name="en-US"/>
```

```
<!-- input preferences -->
 <gs:InputPreferences>
 <gs:InputLanguageID Action="add" ID="0409:00000409"/>
 <gs:InputLanguageID Action="remove" ID="0409:00000409"/>
 </gs:InputPreferences>

<!-- user locale -->
 <gs:UserLocale>
 <gs:Locale Name="en-US" SetAsCurrent="true" ResetAllSettings="false">
 <gs:Win32>
 <gs:iCalendarType>1</gs:iCalendarType>
 <gs:iCurrency>3</gs:iCurrency>
 <gs:iCurrDigits>1</gs:iCurrDigits>
 <gs:sList>...</gs:sList>
 <gs:sDecimal>;;</gs:sDecimal>
 <gs:sThousand>::</gs:sThousand>
 <gs:sGrouping>1</gs:sGrouping>
 <gs:iDigits>2</gs:iDigits>
 <gs:iNegNumber>2</gs:iNegNumber>
 <gs:sNegativeSign>(</gs:sNegativeSign>
 <gs:sPositiveSign>=</gs:sPositiveSign>
 <gs:sCurrency>kr</gs:sCurrency>
 <gs:sMonDecimalSep>,,</gs:sMonDecimalSep>
 <gs:sMonThousandSep>...</gs:sMonThousandSep>
 <gs:sMonGrouping>3</gs:sMonGrouping>
 <gs:iNegCurr>3</gs:iNegCurr>
 <gs:iLZero>0</gs:iLZero>
 <gs:sTimeFormat>:HH:m:s tt:</gs:sTimeFormat>
 <gs:s1159>a.m.</gs:s1159>
 <gs:s2359>p.m.</gs:s2359>
 <gs:sShortDate>d/M/yy</gs:sShortDate>
 <gs:sLongDate>dddd, MMMM yyyy</gs:sLongDate>
 <gs:iFirstDayOfWeek>6</gs:iFirstDayOfWeek>
 <gs:iFirstWeekOfYear>2</gs:iFirstWeekOfYear>
 <gs:sNativeDigits>0246813579</gs:sNativeDigits>
 <gs:iDigitSubstitution>1</gs:iDigitSubstitution>
 <gs:iMeasure>0</gs:iMeasure>
 <gs:iTwoDigitYearMax>2021</gs:iTwoDigitYearMax>
 </gs:Win32>
 </gs:Locale>
 </gs:UserLocale>
 </gs:GlobalizationServices>
```

Syntax

- UserList - This setting specifies the user account for which we need to do the change settings. CopySettingsToDefaultUserAcct and CopySettingsToSystemAcct are the parameters that can be used to copy the settings to all users and also the system account(logonUI screen)

- GeoID/Location Preferences - Updates the current location field under the location tab. Some software, including Windows may provide additional information passed on this, such as weather
- MUILanguagePreference - Supports setting the display language and, if appropriate, the display language fallbacks for the system. Set by using a child element <gs:MUILanguage> with an attribute containing the language string. To set the fallback language of the language set using <gs:MUILanguage>, use the element <gs:MUIFallback>. Using this XML entity does NOT install the display languages. It should only be used for selecting display languages after they have been installed.
- SystemLocale - This setting enables programs that do not use Unicode to run and display menus and dialog boxes in the localized language. If a localized program does not display correctly on the computer, setting the system locale to match the language of the localized program may resolve the problem. However, this setting is system-wide, so it is not possible to support simultaneously the localized programs that do not use Unicode for multiple languages.
- InputPreferences - This setting specifies the input locale and keyboard layout combinations. Note: Unlike in 2003/XP, for some complex languages, the usage of KLIDs to identify keyboard layouts have been replaced by GUIDs. The following link gives a table for the replacement: From KLID to GUID (aka KLIDoral stimulation, it feels GUID)
- UserLocale - This setting controls the settings for sorting numbers, time, currency, and dates. To use .xml answer file to set language preferences:

1. Create an xml file with the required settings and save it as a file (for example: c:\unattend.xml). The .xml file should at minimum include the following:

```
XML

<gs:GlobalizationServices xmlns:gs="urn:longhornGlobalizationUnattend">
 <gs:UserList>
 <gs:User UserID="Current"/>
 </gs:UserList>
 </gs:GlobalizationServices>
```

2. Create a batch file by using the following command line to apply the answer file settings:

```
control.exe intl.cpl,,/f:"c:\Unattend.xml"
```

References

Guide to Windows Vista Multilingual User Interface
https://technet.microsoft.com/library/cc721887(WS.10).aspx

Cannot enter UEFI firmware setup when in native UEFI mode in Windows 7 and Windows 8

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where you can't enter UEFI firmware setup when in native UEFI mode.

Applies to: Windows 10 - all editions
Original KB number: 2804597

Symptoms

Consider the following scenario:

- You enter UEFI F/W setup by pressing F1 key during POST.
- Navigate to **Startup** page and change the **UEFI/Legacy Boot** setting from **Both** to **UEFI Only**.
- Exit UEFI F/W setup using F10 key to save your changes.
- You then boot the system from the Windows 7/Windows 8 installation DVD and do a normal installation.

After Windows 7/Windows 8 setup completes, you're no longer able to enter the UEFI F/W setup option when using the F1 key during POST.

> **Note**
>
> This only impacts certain OEM systems that shipped with Windows 7/Windows 8 preinstalled in BIOS Legacy Boot mode.

Cause

During Windows 7/Windows 8 setup, certain BCDEdit commands will be executed to configure the new installation. These commands may delete information in the BCD store that is necessary for the UEFI boot manager to load the UEFI firmware menu. Also, Vista, Windows Server 2008, Windows 7, Windows 8, or Windows Server 2008 R2 and Windows Server 2012 may modify the BCD store in a way that prevents the UEFI firmware menu from loading.

Resolution

Contact your hardware vendor to see if there is a firmware update available to resolve this issue.

More information

LOAD_OPTION_CATEGORY_APP bit of Attributes in Boot#### is deleted by `bcdedit.exe /export`, then `bcdedit.exe /import /clean` process. It may also be cleared by installing Windows Vista or later. This can cause the UEFI Boot Manager failure to enter UEFI firmware menu.

Erroe after you turn off a Windows 10-based computer from Audit mode: Your account has been disabled

Article • 09/23/2021 • 2 minutes to read

This article helps fix an error (our account has been disabled) that occurs after you turn off a Windows 10-based computer from Audit mode.

Applies to: Windows 10 - all editions
Original KB number: 3141410

Symptoms

Consider the following scenario:

- You're working on a Windows 10-based computer.
- You go into Sysprep Audit mode from the Out of Box Experience (OOBE) screen.
- You turn off the computer by using the **Shut down** command on the **Start** menu, or you use one of the following **Shut down** options:
  - Log off
  - Sleep
  - Hibernate
- You restart or wake the computer.

In this scenario, you receive the following error message on the logon screen:

> Your account has been disabled. Please see your system administrator.

Cause

This is expected behavior because the system is using *hybrid shutdown* (also known as fast startup) during Audit mode. Hybrid shutdown was introduced in Windows 8. In Audit mode, the administrator account is enabled immediately before logoff and disabled immediately after logon. Therefore, the account is locked out when you turn off the computer and then turn it back on.

Workaround

To work around this behavior, disable hybrid shutdown. To do this, follow these steps:

1. Right-click the **Start** button, and then click **Command Prompt (Admin)**.
2. At the command prompt, type the following command, and then press Enter:

```
Console

shutdown /s /t 00
```

Computer screen goes black during the Windows 7 installation process

Article • 09/23/2021 • 3 minutes to read

This article provides a solution to an issue where a black screen is displayed during Windows 7 setup on systems with embedded DisplayPort from AMD/ATI.

Applies to: Windows 7 Service Pack 1
Original KB number: 978226

> **Note**
>
> This article is intended for advanced computer users. If you purchased a retail copy of Windows 7, click the support link on the right side of your screen.

Symptoms

Your computer has an AMD/ATI Radeon graphics processing unit (GPU) that uses the embedded DisplayPort (eDP) technology. When you install Windows 7 on the computer, a black screen is displayed during the installation process. However, the installation is still running. In this situation, you may be unable to complete the installation.

> **Note**
>
> If you have multiple displays, only the primary screen is black when you encounter this issue.

Cause

AMD implemented eDP support after the Windows 7 DVD was finished. Therefore, the AMD Radeon graphics driver on the Windows 7 retail DVD does not support eDP.

AMD has released an updated driver that fixes the eDP issue. The update must be incorporated into the setup process for setup to complete successfully.

Resolution

To resolve this problem, follow these steps:

1. Save the Autounattend.xml answer file and the latest graphics driver to a USB flash drive. To do this, follow these steps:
   a. Copy an Autounattend.xml file to the root of a USB flash drive. If you want to create an Autounattend.xml file yourself, go to the Create an Autounattend.xml file section.
   b. Copy the uncompressed graphics driver onto the USB flash drive. To do this, follow these steps:

      i. Download the latest driver for your graphics adapter from the AMD Web site.

      ii. Run the downloaded program (.exe) to extract the driver. The program will prompt for an installation location, such as c:\ati\support.

      iii. After the extraction is complete, locate the installation folder that is noted in the previous step.

      iv. Copy the installation folder onto the USB flash drive.

2. From the Windows 7 installation DVD, start the computer that has the AMD Radeon GPU that uses eDP.

3. Immediately connect the USB flash drive after the computer starts from DVD.

4. Follow the instructions to complete the installation process.

5. When the system restarts for the first time, disconnect the USB flash drive.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Workaround

If you have a secondary monitor, connect the monitor to the computer before you install Windows 7. Then, you will be able to complete the setup process. After Windows 7 is installed, you can install an updated driver that corrects the eDP issue through Windows Update or through the AMD Web site.

Affected systems

The issue is known to occur with the following system:

- Apple iMac 27"

The issue also affects systems that have one of the following AMD/ATI Radeon GPU's:

- ATI Mobility Radeon HD 4650 (PCI\VEN_1002&DEV_9480)
- ATI Mobility Radeon HD 4670 (PCI\VEN_1002&DEV_9488)
- ATI Mobility Radeon HD 4870 (PCI\VEN_1002&DEV_945A)
- ATI Mobility Radeon HD 4850 (PCI\VEN_1002&DEV_944A)
- ATI Mobility Radeon HD 4330 (PCI\VEN_1002&DEV_9552)

Create an Autounattend.xml file

To create an Autounattend.xml file yourself, follow these steps:

1. On any computer that you can use, start Notepad, and then paste the following text in the Notepad window:

XML

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
     <servicing></servicing>
     <settings pass="windowsPE">
         <component name="Microsoft-Windows-PnpCustomizationsWinPE"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
             <DriverPaths>
                 <PathAndCredentials wcm:keyValue="1" wcm:action="add">
                     <Path>%configsetroot%</Path>
                 </PathAndCredentials>
             </DriverPaths>
         </component>
         <component name="Microsoft-Windows-Setup"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
             <UseConfigurationSet>true</UseConfigurationSet>
         </component>
         <component name="Microsoft-Windows-PnpCustomizationsWinPE"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
             <DriverPaths>
                 <PathAndCredentials wcm:keyValue="1" wcm:action="add">
```

```
                    <Path>%configsetroot%</Path>
                </PathAndCredentials>
            </DriverPaths>
        </component>
        <component name="Microsoft-Windows-Setup"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <UseConfigurationSet>true</UseConfigurationSet>
        </component>
    </settings>
    <settings pass="offlineServicing">
        <component name="Microsoft-Windows-PnpCustomizationsNonWinPE"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <DriverPaths>
                <PathAndCredentials wcm:keyValue="2" wcm:action="add">
                    <Path>%configsetroot%</Path>
                </PathAndCredentials>
            </DriverPaths>
        </component>
        <component name="Microsoft-Windows-PnpCustomizationsNonWinPE"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <DriverPaths>
                <PathAndCredentials wcm:keyValue="2" wcm:action="add">
                    <Path>%configsetroot%</Path>
                </PathAndCredentials>
            </DriverPaths>
        </component>
    </settings>
    <settings pass="auditSystem">
        <component name="Microsoft-Windows-PnpCustomizationsNonWinPE"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <DriverPaths>
                <PathAndCredentials wcm:keyValue="3" wcm:action="add">
                    <Path>%configsetroot%</Path>
                </PathAndCredentials>
            </DriverPaths>
        </component>
        <component name="Microsoft-Windows-PnpCustomizationsNonWinPE"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <DriverPaths>
                <PathAndCredentials wcm:keyValue="3" wcm:action="add">
```

```
                    <Path>%configsetroot%</Path>
                </PathAndCredentials>
            </DriverPaths>
        </component>
    </settings>
    <cpi:offlineImage cpi:source="wim:d:/sources/install.wim#Windows 7
ULTIMATE" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
</unattend>
```

2. Save the file as **Autounattend.xml** by using the UTF-8 encoding format.

References

For more information about unattended installations, see Windows Automated Installation Kit for Windows 7.

Customize the default local user profile when you prepare an image of Windows

Article • 09/23/2021 • 9 minutes to read

This article describes how to customize the default local user profile settings when you create an image in Windows 7.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 973289

Summary

After you deploy the image, the default local user profile settings are applied to all new users who log on to the computer.

To customize a default user profile or a mandatory user profile, you must first customize the default user profile. Then, the default user profile can be copied to the appropriate shared folder to make that user profile either the default user profile or a mandatory user profile.

When the default user profile is customized as described in this article, it reconstructs the source profile in a format that is appropriate for use by multiple users. This is the only supported method of customizing the default user profile for the Windows operating system. If you try to use other methods to customize the default user profile, it may result in extraneous information being included in this new default user profile. Such extraneous information could lead to serious problems with applications and system stability.

This article supersedes all previously published procedures about how to customize default local user profiles when you prepare images.

Customize a default user profile

The only supported method for customizing the default user profile is by using the `Microsoft-Windows-Shell-Setup\CopyProfile` parameter in the Unattend.xml answer file. The Unattend.xml answer file is passed to the System Preparation Tool (Sysprep.exe).

Step 1: Configure the default user profile

1. Log on to Windows by using the built-in local Administrator account.

   > **Note**
   >
   > You cannot use a domain account for this process.

2. Open the User Accounts control panel, and remove all added user accounts except for the one Administrator-level user account that you used to log on to Windows.

3. Configure the settings that you want to copy to the default user profile. This includes desktop settings, favorites, and **Start** menu options.

   > **Note**
   >
   > Customizing the **Start** menu and the **Taskbar** is limited in Windows 7.

Step 2: Create an Unattend.xml file that contains the Copy Profile parameter

Create an Unattend.xml file that contains the Copy Profile parameter (`Microsoft-Windows-Shell-Setup\CopyProfile`). By using this Copy Profile parameter, the settings of the user who is currently logged on are copied to the default user profile. This parameter must be set to **true** in the specialize pass.

Windows System Image Manager (Windows SIM) creates and manages unattended Windows Setup answer files in a graphical user interface (GUI).

Answer files are XML-based files that are used during Windows Setup to configure and to customize the default Windows installation.

Use the Windows System Image Manager tool to create the Unattend.xml file. The Windows System Image Manager tool is included as part of the Windows Automated Installation Kit (Windows AIK). Obtain the AIK for your operating system from one of the following websites:

- Windows Automated Installation Kit (AIK) for Windows Vista
- Automated Installation Kit (AIK) for Windows Vista SP1 and Windows Server 2008
- The Windows Automated Installation Kit (AIK) for Windows 7 and Windows Server 2008 R2

- The Windows Automated Installation Kit (AIK) Supplement for Windows 7 SP1 and Windows Server 2008 R2 SP1

For more information about Windows AIK, see Windows Automated Installation Kit (AIK). Directions about how to create an answer file can be found in the Help information that is included with Windows AIK. For more information about how to create an answer file, see Work with Answer Files in Windows SIM.

Step 3: Customize the default user profile in the Unattend.xml file

1. Open an elevated command prompt. To do this, click **Start**, type *cmd* in the **Search** box, right-click cmd in the Programs list, and then click **Run as administrator**.

   If you are prompted for an administrator password or for confirmation, type the password or provide confirmation.

2. At the command prompt, type the following command, and then press ENTER:

   Console

   ```
   %systemroot%\system32\sysprep\sysprep.exe /oobe /shutdown /generalize
   /unattend:c:\answerfile\unattend.xml
   ```

   > **Note**
   >
   > Sysprep.exe is located in the `%systemdrive%\Windows\System32\sysprep` directory.

3. To confirm that the CopyProfile command successfully completed, open the `%systemroot%\panther\unattendgc\setupact.log` file.

4. Search for lines that resemble the following (in the specialize pass):

   > [shell unattend] CopyProfileDirectory from c:\Users\Administrator succeeded.
   > [shell unattend] CopyProfile succeeded.

   This line confirms whether the CopyProfile command succeeded and which user profile was copied to the default user profile.

5. Capture the image.

6. Deploy the image. For more information about how to use Sysprep to capture and deploy an image, see Sysprep Technical Reference.

> **Note**
>
> - You must use the `/generalize` switch with sysprep.exe so that the Copy Profile parameter can be used. The `/unattend` option is used to point to the desired Unattend.xml file. Therefore, in this example, the Unattend.xml file is located in the `c:\answerfile` folder.
> - The built-in administrator account profile is deleted when you perform a clean Windows installation or when you run the Sysprep tool. The CopyProfile setting is processed before the built-in administrator account is deleted. Therefore, any customizations that you make will appear in the new user account profile. This includes the built-in administrator account profile settings.
> - If there are multiple user profiles, Windows sysprep may select an unexpected profile to copy to the default user profile.
> - Not all customizations will propagate to new profiles. Some settings are reset by the new user logon process. To configure those settings, use Group Policy settings or scripting.

What to consider if you use automated image build and deployment systems

- When you use tools such as the Microsoft Deployment Toolkit or System Center Configuration Manager, the CopyProfile setting is not required when you run the Sysprep command. These tools usually replace or change the Unattend.xml file after the image is deployed to the disk but before the operating system has started for the first time after you run the Sysprep command. Therefore, the Unattend.xml file that is used in the Microsoft Deployment Toolkit or System Center Configuration Manager deployment process must contain the CopyProfile setting.

- If you set the CopyProfile setting to **true** when you run Setup from the Windows 7 installation media during the image build process, the administrator profile settings may be unintentionally copied into the default user profile. The administrator profile settings are typically present in the Install.wim file on the installation media.

Turn the default user profile into a network default user profile

To turn the default user profile into a network default user profile, follow these steps:

1. Use an account that has administrative credentials to log on to the computer that has the customized default user profile.
2. Use the `Run` command to connect to the NETLOGON shared folder of a domain controller. For example, the path resembles the following: `\\<Server_name>\NETLOGON`
3. Create a new folder in the NETLOGON shared folder, and name it *Default User.v2*.
4. Click **Start**, right-click **Computer**, click **Properties**, and then click **Advanced system settings**.
5. Under **User Profiles**, click **Settings**. The **User Profiles** dialog box shows a list of profiles that are stored on the computer.
6. Select **Default Profile**, and then click **Copy To**.
7. In the **Copy profile to** text box, type the network path of the Windows default user profile folder that you created in step 3. For example, type the path `\\<Server_name>\NETLOGON\Default User.v2`.
8. Under **Permitted to use**, click **Change**, type the name *Everyone*, and then click **OK**.
9. Click **OK** to start to copy the profile.
10. Log off from the computer when the copying process is completed.

Turn the default user profile into a mandatory user profile

You can configure the default local user profile to become a mandatory profile. By doing this, you can have one central profile that is used by all users. To do this, you have to prepare the mandatory profile location, copy the local default user profile to the mandatory profile location, and then configure a user's profile location to point to the mandatory profile.

Step 1: Prepare the mandatory profile location

1. On a central file server, create a new folder or use an existing folder that you use for roaming user profiles. For example, you can use the folder name *Profiles*: `\Profiles`

2. If you are creating a new folder, share the folder by using a name that is suitable for your organization.

   > ⓘ **Note**
   >
   > The share permissions for shared folders that contain roaming user profiles must enable Full Control permissions for the **Authenticated Users** group. The share permissions for folders that are dedicated to storing mandatory user profiles should enable Read permissions for the **Authenticated Users** group and enable Full Control permissions for the **Administrators** group.

3. Create a new folder in the folder that is created or identified in step 1. The name of this new folder should start with the logon name of the user account if the mandatory user profile is for a specific user. If the mandatory user profile is for more than one user, name it accordingly. For example, the following domain has a mandatory profile, and the folder name begins with the word *mandatory*: `\Profiles\mandatory`

4. Finish naming the folder by adding *.v2* after the name. The example that is used in step 3 has the folder name *mandatory*. Therefore, the final name of the following folder for this user is *mandatory.v2*: `\Profiles\mandatory.v2`

Step 2: Copy the default user profile to the mandatory profile location

1. Log on to the computer that has the customized local default user profile by using an account that has administrative credentials.

2. Click **Start**, right-click **Computer**, click **Properties**, and then click **Advanced System Settings**.

3. Under **User Profiles**, click **Settings**. The **User Profiles** dialog box shows a list of profiles that are stored on the computer.

4. Select **Default Profile**, and then click **Copy To**.

5. In the **Copy profile to** text box, type the network path of the Windows default user folder that you created in the Step 1: Prepare the mandatory profile location section. For example, type the following path:
   `\\<Server_name>\Profiles\mandatory.v2`
6. Under **Permitted to use**, click **Change**, type the name *Everyone*, and then click **OK**.
7. Click **OK** to start to copy the profile.
8. Log off from the computer when the copying process is completed.
9. On the central file server, locate the folder that you created in the Step 1: Prepare the mandatory profile location section.
10. Click **Organize**, and then click **Folder options**.
11. Click the **View** tab, click to select the **Show hidden files and folders** check box, click to clear the **Hide extensions for known file types** check box, click to clear the **Hide protected operating system files** check box, click **Yes** to dismiss the warning, and then click **OK** to apply the changes and close the dialog box.
12. Locate and right-click the NTUSER.DAT file, click **Rename**, change the name of the file to NTUSER.MAN, and then press ENTER.

> ⓘ **Note**
>
> Previously it was possible to copy profiles by using the System Control Panel item. This copy to default profile option is now disabled as it could add data that made the profile unusable.

Step3: Prepare a user account

1. As a domain administrator, open the Active Directory Users and Computers management console from a Windows Server 2008 R2 or Windows Server 2008 computer.
2. Right-click the user account to which you want to apply the mandatory user profile, and then click **Properties**.
3. Click the **Profile** tab, type the network path that you created in the Step 1: Prepare the mandatory profile location section in the profile path text box. However, don't add *.v2* at the end. In our example, the path would be as follows:
   `\\<Server_name>\Profiles\mandatory`

4. Click **OK**, and then close the Active Directory Users and Computers management console. The user will now use the customized mandatory user profile.

Still need help

If this article does not answer your question, ask a question and pose it to other community members at Microsoft Community.

Resources

If you are having issues logging on to a user profile, see the website:

- Fix a corrupted user profile
- Create a user account

Download and burn an ISO file on the volume licensing site (VLSC)

Article • 12/06/2021 • 2 minutes to read

This article describes how to download and burn an ISO file from the Microsoft Volume Licensing Service Center (VLSC).

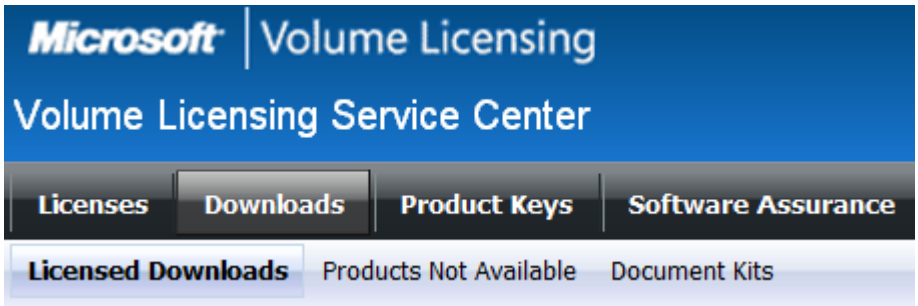
Applies to: General
Original KB number: 2472143

Summary

From the VLSC, you can download software included in your contract. On the section **Downloads** you can find two types, EXE & ISO files. An ISO file should be saved into a CD or DVD through a burning software.

Download and burn an ISO file

1. Access the Volume License Service Center (VLSC).
2. Enter your Windows Live ID E-mail address and password, then select the **Sign-In** button.
3. Select **Downloads** > **Licensed Downloads**, and then search for your product.



4. Choose the Download Settings from the drop-down box. Specify the **Language** and **Connection Speed**. **Operating System Type** may be required for certain products.



5. Select **Continue Download**.

6. You may choose either **Download Manager** or the **Web Browser**.

   a. Download Manager is a program to pause and resume the download at any time by selecting the **Pause** button. You can cancel the download if required by clicking the **Cancel** button.

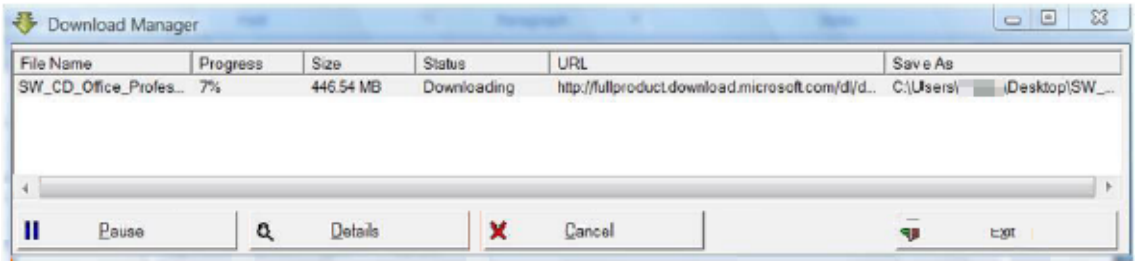
Download Format	(Recommended) Download Manager	Web Browser
EXE	Download	Download
ISO	Download	Download

   b. Choose the location on your computer and select the **Save** button.

> ⓘ **Note**
>
> You will be prompted to install the Download Manager on your first download.

   c. The Download Manager opens and the download begins.

   d. You can cancel the download if required by clicking the **Cancel** button.



7. The ISO file should be saved on the hard disk on your computer.

8. When the download is completed, copy the ISO file to a CD or DVD using a software burning program.

9. This CD or DVD can then be used to install the ISO software.

References

- Create installation media for Windows

- Volume Licensing Service Center

Error 0x80042468 when creating a single partition on a drive greater than 2.2 TB during install of Windows

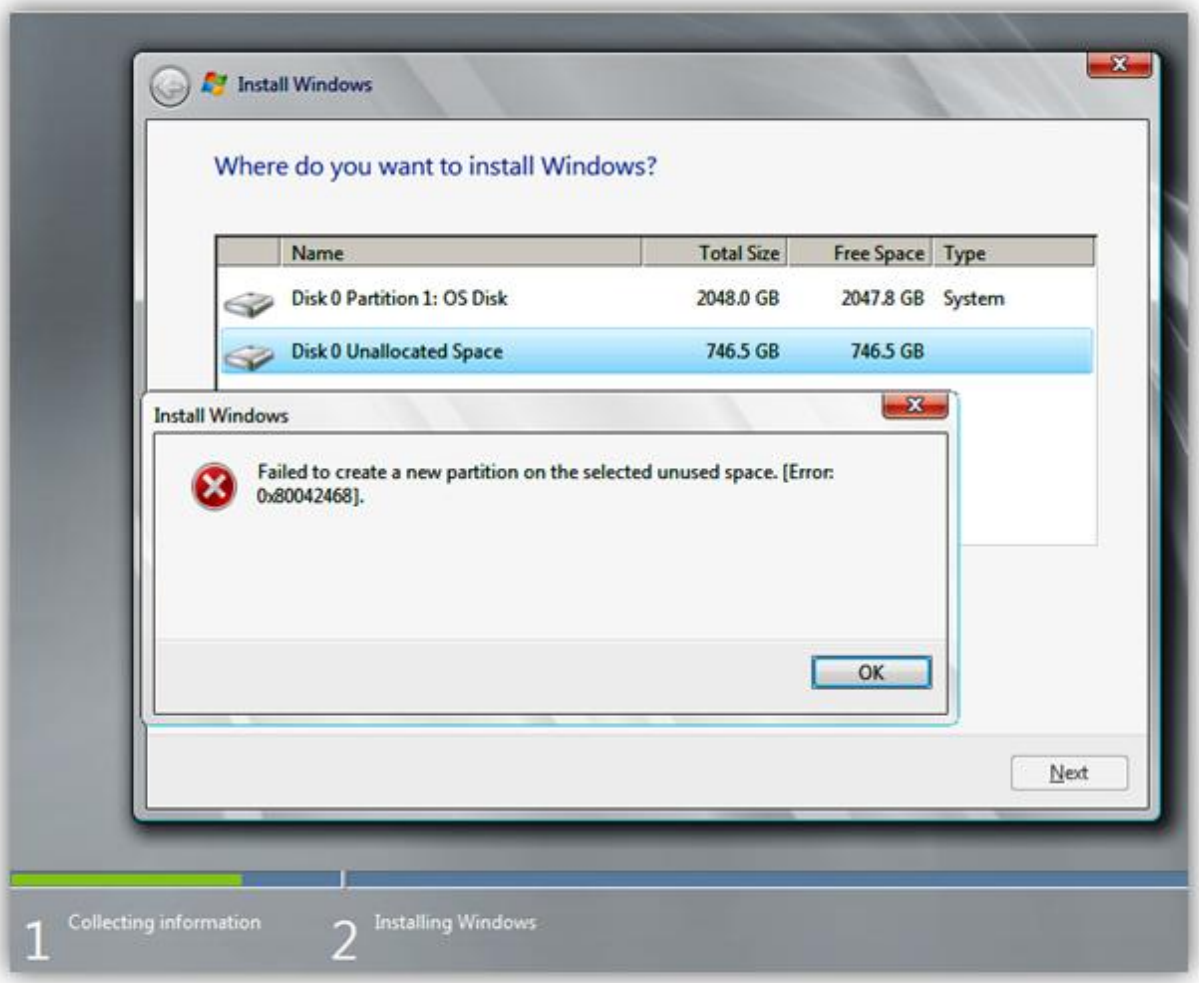
Article • 12/06/2021 • 2 minutes to read

This article provides a solution to an error that occurs when you install Windows to a drive greater than 2.2 TB.

Applies to: Windows 7 Service Pack 1
Original KB number: 2604034

Symptoms

When installing Windows to a drive greater than 2.2TB, you receive Error 0x80042468. This will occur if you install Windows 7 and manually try to create one partition using "Advanced Drive Options" during setup.



Cause

It's by design with Windows 7 x86 and with Windows 7 x64 on a non-UEFI system.

> ⓘ **Note**
>
> The check for UEFI (Unified Extensible Firmware Interface) and GUID Partition Table (GPT) isn't done during Setup in Advanced Format like it's done in Disk Management.

Resolution

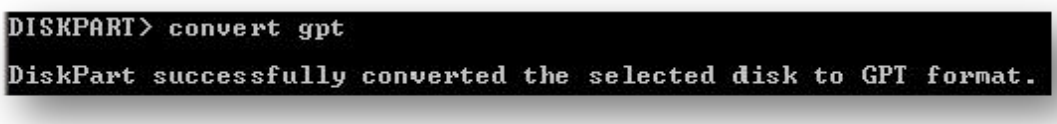
Install will complete but you won't be able to access the drive beyond 2.2 TB.

If you install Windows 7 x64 on a system that supports UEFI, you can partition the drive to use GUID Partition Table (GPT) and access all of the drive if the system is in UEFI mode.

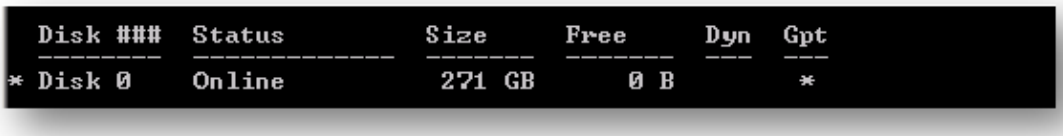
> ⓘ **Important**
>
> The disk that you select can't contain any data. Back up the data, or move your data to another volume before doing operations in diskpart.

To Boot a UEFI enabled system, the disk type should be changed to GPT using convert gpt command. Follow steps as below.

1. Press Shift+F10, which brings a command window. At command prompt, run the Diskpart.exe (It starts the diskpart console. After the console is initialized, DISKPART> is displayed. The diskpart console is now ready for input commands.)
2. Under diskpart> prompt type "list disk". (Locate the disk, in this case disk 0)
3. Type **Select disk 0** (It selects the disk that you want to convert to GPT.)
4. Type **Convert GPT** (This command will convert drive to GPT.)



5. Just to make sure everything went fine type **list disk**. The converted disk should now have an asterix in the GPT column. (See example image below)



6. Type exit and exit again. It should close the command window.

Select the disk you have converted and that should display as **Unallocated Space**.

The installation process should start and continue as usual. After reboot, the Windows 7 x64 should be installed on the GPT partitioned disk.

More information

Windows doesn't support booting of GPT initialized volumes with UEFI systems on 32-bit versions of Windows, and that legacy BIOS (Basic Input/Output System) systems don't support booting of GPT partitioned volumes. Consult with your system vendor to determine if the system supports UEFI and booting of devices greater than 2 TB.

For details on Windows support for large drives, see the following articles:

- Windows support for hard disks that are larger than 2 TB
- How to establish and boot to GPT mirrors on 64-bit Windows
- Configure UEFI/GPT-Based Hard Drive Partitions
- Using GPT Drives

Event ID 10 is logged in the Application log after you install Service Pack 1 for Windows 7 or Windows Server 2008 R2

Article • 09/23/2021 • 2 minutes to read

This article provides a script to solve the event ID 10 that's logged after you install Service Pack 1 for Windows 7 or Windows Server 2008 R2.

Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
Original KB number: 2545227

Symptoms

After you install Windows 7 Service Pack 1 (SP1) or Windows Server 2008 R2 SP1 using integrated media, the following WMI error is logged in the application log after every reboot:

Output

```
Log Name - Application
Source - WMI
EventID - 10
Level - Error
User - N/A
OpCode - Info
Task Cat - None
Keywords - Classic
Details - Event filter with query "SELECT * FROM __InstanceModificationEvent
WITHIN 60 WHERE TargetInstance ISA "Win32_Processor" AND
TargetInstance.LoadPercentage > 99" could not be reactivated in namespace
"//./root/CIMV2" because of error 0x80041003. Events cannot be delivered
through this filter until the problem is corrected.
```

Cause

This issue originated in the Windows 7 SP1 DVD/ISO creation process. There was an issue in the creation process that caused a WMI registration to remain in the DVD/ISO. Since the registration is designed to work only during the DVD/ISO creation process, it fails to run on a live system and causes these events. These events aren't indicative of any issue in the system and can be safely ignored. If you want to prevent these events

from getting generated and want to remove this specific WMI registration manually, run the workaround script.

Resolution

To resolve the issue, run a script to stop the Event ID 10 messages. To run the script, follow these steps:

1. In Notepad, create a new document named *Workaround.txt*.
2. Copy the following script into notepad:

```VB
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
& "{impersonationLevel=impersonate}!\\" _
& strComputer & "\root\subscription")
Set obj1 = objWMIService.ExecQuery("select * from __eventfilter where
name='BVTFilter' and query='SELECT * FROM __InstanceModificationEvent
WITHIN 60 WHERE TargetInstance ISA ""Win32_Processor"" AND
TargetInstance.LoadPercentage > 99'")
For Each obj1elem in obj1
set obj2set = obj1elem.Associators_("__FilterToConsumerBinding")
set obj3set = obj1elem.References_("__FilterToConsumerBinding")
For each obj2 in obj2set
WScript.echo "Deleting the object"
WScript.echo obj2.GetObjectText_
obj2.Delete_
next
For each obj3 in obj3set
WScript.echo "Deleting the object"
WScript.echo obj3.GetObjectText_
obj3.Delete_
next
WScript.echo "Deleting the object"
WScript.echo obj1elem.GetObjectText_
obj1elem.Delete_
Next
```

3. Save the text as *Workaround.vbs*.
4. Close Notepad.
5. Open an elevated command prompt:
   a. Select **Start**.
   b. Select **Programs**.
   c. Right-click on **Command Prompt**.

d. Choose **run as administrator**.

6. Change Directory to the one containing *workaround.vbs*, for example, `CD c:\users\%username%`.

7. Run the script *workaround.vbs*.

After running the script, the Event ID 10 errors related to this event should stop occurring. This script doesn't remove any of the existing entries in the Event log, they would need to be manually cleared out of the application event log.

> ⓘ **Note**
>
> There can be other reasons for Event ID 10 error messages. This workaround only prevents the error message listed above from occurring.

More information

This particular Event ID 10 error message listed above can be safely ignored. It isn't indicative of a problem with the Service Pack or with the operating system.

F5 doesn't refresh Explorer in Windows PE of Windows 10 Creators Update

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround to the issue in which F5 doesn't refresh Explorer in Windows PE of Windows 10 Creators Update.

Applies to: Windows 10, version 1903, Windows 10, version 1809
Original KB number: 4033241

Symptoms

Consider the following scenario:

- You start Windows 10 in Windows Preinstallation Environment (PE) mode.
- You create a folder or rename a folder.
- You press the F5 key.

In this scenario, the folder and file list do not refresh.

Workaround

To refresh the files, use one of the following methods:

- Click another folder, and then click the previous folder.
- Move the mouse cursor over the folder and file list.

"Windows could not parse or process the unattend answer file for pass [specialize]" error message when you perform an in-place upgrade

Article • 09/23/2021 • 2 minutes to read

This article provides help to fix an error (Windows could not parse or process the unattend answer file for pass [specialize]) that occurs when you perform an in-place upgrade.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2425962

Symptoms

Consider the following scenario:

- You are running a version of Windows 7 or of Windows Server 2008 R2 that was installed by using an Unattend.xml file.
- You start the computer from this image, and then you select the **Repair in-place upgrade (overwrite installation)** option.
- You start the in-place upgrade.

In this scenario, you receive the following error message: Windows could not parse or process the unattend answer file for pass [specialize].

Generally, the Unattend.xml files are used for OEM or corporate environment deployment. Therefore, the image could contain an Unattend.xml file, and you may not be aware that this file is included.

Cause

This problem occurs because the Unattend.xml file is applied during the in-place upgrade. This scenario is not supported.

More information

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base: 322756 How to back up and restore the registry in Windows

When this behavior occurs, you cannot recover the system. Therefore, you must perform a clean installation.

To avoid this behavior, you can remove a registry subkey before you use the OEM installation image to run an in-place upgrade. To do this, follow these steps:

1. Log on to the computer by using a user account that has administrative permissions.
2. Click **Start**, type **regedit** in the **Start search** box, and then in the **Programs** list, click **regedit.exe**.
3. Locate and then right-click the following registry subkey:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\UnattendBackup\ActiveSetup\FavoritesList\Favorite<XX>

   > **Note**
   >
   > In this subkey, <**XX**> is a placeholder for numbers that begin with 1.
4. Click **Delete**, click **Yes**, and then exit Registry Editor.

Status

This behavior is by design.

Error (BlInitializeLibrary failed XXX) when you install or start an operating system on a 64-bit UEFI-based computer

Article • 03/04/2022 • 2 minutes to read

This article provides a workaround for an issue where an error (BlInitializeLibrary failed XXX) occurs when you install or start an operating system on a 64-bit UEFI-based computer.

Applies to: Windows 10 - all editions, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2
Original KB number: 4020050

Symptoms

When you try to install or start an operating system on a 64-bit UEFI-based computer, the system does not start, and you receive the following error message:

> BlInitializeLibrary failed XXX

> **Note**
>
> The error code could also be 0xc000009a or 0xc0000001.

Cause

This problem occurs because the boot firmware on the computer generates lots of memory fragmentation.

> **Note**
>
> Not all "BlInitializeLibrary failed XXX" errors are caused by this issue.

Workaround

We recommend that you do not let boot firmware create large amounts of fragmentation. Large memory fragmentation degrades the overall startup performance and causes problems.

More information

At the pre-boot stage, Windows Boot Manager sets the maximum number of global memory descriptor for a 64-bit UEFI system at 512. If the boot firmware creates a large amount of memory fragmentation, the memory descriptor count may exceed the set limit. This causes the "BlInitializeLibrary failed XXX" error.

> **Note**
>
> This design applies only to the current operating system releases, including Windows 10, Windows Server 2016, and Windows Server 2012 R2. We do not guarantee that this design will apply to future versions.

Error during Windows 10 upgrade: Contact your system administrator to upgrade Windows Server or Enterprise Editions

Article • 09/23/2021 • 2 minutes to read

This article provides help to fix an error that occurs during Windows 10 upgrade: Contact your system administrator to upgrade Windows Server or Enterprise Editions.

Applies to: Windows 10 - all editions
Original KB number: 3188105

Symptoms

When you run the updater tool from the Get the anniversary Update Now link at Windows 10 update history, you receive the following error message:

> Windows 10 will not run on this PC
> Operating system: "Contact your system administrator to upgrade Windows Server or Enterprise Editions"

Cause

The tool works only with the Windows 10 Home, Pro, and Education editions. If you're running the Windows 10 Enterprise edition, you receive the error message.

Resolution

To resolve this issue, use a different method to upgrade to Windows 10 version 1607. For example, download the ISO, and then run Setup from it.

Error HAL_INITIALIZATION_FAILED when you install Windows 8 or Windows Server 2012 on VMware VM

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to fix a HAL_INITIALIZATION_FAILED error that occurs when you install Windows 8 or Microsoft Windows Server 2012 on VMware VM.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2814803

Symptoms

Consider the following scenarios:

Scenario 1

When installing Windows 8, Windows Server 2012, or booting using Windows PE 4.0 on a VMware 4.x virtual machine running a Windows operating system, you may encounter the following error:

> Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you. (0% complete)
> If you would like to know more, you can search online later for this error: HAL_INITIALIZATION_FAILED

Note

If you attempt to boot the x86 version of Windows PE 4.0, the system will hang.

Scenario 2

You attempt to execute an Offline P2V using System Center Virtual Machine Manager 2012 SP1 for a virtual machine (Windows operating system) running on a VMware ESX server 4.x, you experience the symptoms as mentioned in the Scenario 1.

Scenario 3

Assume that you install Windows 8 or Windows Server 2012 on a VMware virtual machine. In this situation, the VM crashes while booting and you may receive the following Stop error code:

> STOP: 0x0000005D (parameter1, parameter2, parameter3, parameter4)

Cause

VMware 4.x doesn't support Windows 8 or Windows Server 2012 as guest operating system. VMware 4.x also doesn't support an Offline P2V of a virtual machine running a Windows operating system when using System Center Virtual Machine Manager (VMM) 2012 SP1. This version of VMM uses WinPE 4.0 when executing the Offline P2V process.

Resolution

Upgrade to later version of VMware (at least version 5.1). For Scenario 2, the options include:

1. Execute an Online P2V. This option may not be recommended for some virtual machines, such as those functioning as Domain Controllers, and or SQL servers.
2. Execute a V2V
3. Use the Microsoft Virtual Machine Converter solution - Microsoft Virtual Machine Converter

More information

You can also run into this issue in other scenarios involving WDS, SCCM, or other deployment technologies. For example, attempting to PXE boot a Windows 8 boot.wim.

For more information on support for Windows 8 and Windows Server 2012 in VMware, see the following article:
Windows 8 / Windows Server 2012 Operating System does not boot or install on ESXi or ESX (2006859) .

For more information on support for operating systems in VMware Guests, see the following article:
VMware Compatibility Guide .

Hardware requirements for Windows 8 and Windows Server 2012:
PAE/NX/SSE2 Support Requirement Guide for Windows 8

How to customize the default local user profile when you prepare an image of Windows

Article • 09/23/2021 • 3 minutes to read

This article discusses how to customize the default local user profile settings when you create an image in Windows.

Applies to: Windows 10 – all editions, Windows Server 2012 R2
Original KB number: 959753

Introduction

This article discusses how to customize the default local user profile settings when you create an image on a computer that is running one of the following operating systems:

- Windows XP
- Windows Server 2003

After you deploy the image, these settings are applied to all new users who log on to the computer.

> **Note**
>
> This article supersedes all previously published procedures for customizing default local user profiles when you prepare images.

For more information about the steps to customize the default local user profile for Windows Vista or later operating systems, see How to customize default user profiles in Windows Vista, Windows Server 2008, Windows 7, and in Windows Server 2008 R2.

How to customize the default local user profile in Windows XP or in Windows Server 2003

In Windows XP and in Windows Server 2003, updates that you've installed may change the method that you use to customize the default local user profile. For more information, see the following sections.

Windows XP Service Pack 2 (SP2)

The default behavior is to automatically copy customizations from the administrator profile to the default user profile. Therefore, no additional steps are required to customize the profile.

Windows Server 2003 Service Pack 1 (SP1) or Windows Server 2003 SP2

The default behavior is to automatically copy customizations from the administrator profile to the default user profile. Therefore, no additional steps are required to customize the profile. You can disable this functionality by setting a parameter in the Sysprep.inf file. This parameter prevents the Minisetup process from copying customizations from the administrator profile. To do this, set the parameter in the "UNATTENDED" section of the Sysprep.inf file as follows:

```
INF

[UNATTENDED]
UpdateServerProfileDirectory=0
```

Windows XP Service Pack 3 (SP3) or hotfix 887816 is applied

Hotfix 887816 disables the automatic copying of customizations. Therefore, you must configure a parameter in the Sysprep.inf file to enable the Minisetup process to copy the customizations from the administrator profile. To do this, set the parameter in the "UNATTENDED" section, as follows:

```
INF

[UNATTENDED]
UpdateServerProfileDirectory=1
```

> **Note**
>
> Windows XP SP3 includes hotfix 887816.

Windows XP or Windows Server 2003

To use this CopyProfile setting in Windows XP SP2 together with hotfix 887816, in Windows XP SP3, or in Windows Server 2003 SP1, the UpdateServerProfileDirectory setting must be present in the Sysprep.inf file when you run the Sysprep tool. Therefore, when you use automated image build and deployment tools, such as the Microsoft Deployment Toolkit or System Center Configuration Manager, the UpdateServerProfileDirectory setting must be included during the reference image build and capture process.

References

For more information about how to configure default local user profile settings, visit the following Microsoft website:

Configuring Default User Settings – Full Update for Windows 7 and Windows Server 2008 R2

More information

The procedure that is described in this article supersedes all previously published procedures for customizing default local user profiles when you prepare images. This behavior applies to the following operating systems:

- Windows Server 2003
- Windows XP

Previously published procedures relied on a file copy mechanism. These procedures caused information to be left behind in the default user profile that caused the Windows shell to behave incorrectly. This led to problems with application compatibility and with the user experience. Therefore, don't advise customers to copy profiles over the default user profile. This method is no longer supported.

How to configure the default network profile

Install the version of Windows for which you want to use the profile. Follow the procedures in this article to configure the local default user profile. Restart the computer after you run the Sysprep command. When the operating system finishes the Minisetup/Specialize process, log on as the local administrator. Use the newly configured local default user profile as the source for the default network profile.

How to configure default user settings for already deployed desktops

Implement the required new or changed settings as a logon script and configure it to run one time.

You can automate the procedure in Knowledge Base article 284193 by using the Reg.exe command. For an alternative solution, see the "Targeted changes to the Default User Registry hive and profile folders" section on the following Microsoft website:

Configuring Default User Settings – Full Update for Windows 7 and Windows Server 2008 R2

How to edit the Boot.ini file in Windows 2000

Article • 09/23/2021 • 3 minutes to read

This article describes the steps to edit the Boot.ini file in a Windows 2000 environment.

> **Note**
>
> This article applies to Windows 2000. Support for Windows 2000 ends on July 13, 2010. The Windows 2000 End-of-Support Solution Center is a starting point for planning your migration strategy from Windows 2000. For more information, see the **Microsoft Support Lifecycle Policy**.

Applies to: Windows 2000
Original KB number: 311578

Summary

This step-by-step article describes how to edit the Boot.ini file in a Windows 2000 environment. NTLDR displays the bootstrap loader screen, where you can select an operating system to start. This screen is based upon the information in the Boot.ini file. If you don't select an entry before the counter reaches zero, NTLDR loads the operating system that is specified by the default parameter in the Boot.ini file. Windows 2000 Setup places the Boot.ini file in the active partition. NTLDR uses information in the Boot.ini file to display the bootstrap loader screen from which you select the operating system.

You should back up the Boot.ini file before you edit it. The first tasks include modifying your folder options so you can view hidden files, and then backing up the Boot.ini file.

Modifying Folder Options

1. Right-click Start, and then click Explore.
2. On the Tools menu, click Folder Options, and then click View.
3. In the Advanced Settings area, click to select the **Show hidden files and folders** check box, click to clear the **Hide protected operation system files (Recommended)** check box, click OK, and then click OK.

4. In the left pane, click to select the %systemroot%, right-click Boot.ini in the display pane, and then click Properties.
5. Click to clear the Read-only attribute check box, and then click OK.

Save a backup copy of Boot.ini

1. Right-click Start, and then click Explore.
2. In the left pane, click the %systemroot% drive, in the right pane, click the Boot.ini file, and then click Copy.
3. Open a temporary folder in the left pane, right-click in the right display pane, and then click Paste to create a copy of the Boot.ini file in that folder.

Sample Boot.ini file

This is a sample of a default Boot.ini file from a Windows 2000 Server-based computer:

ini

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows 2000 Server" /fastdetect
```

This is a sample of the preceding Boot.ini file after the addition of another partition that is running Windows XP Professional.

ini

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows 2000 Server" /fastdetect
multi(0)disk(0)rdisk(0)partition(2)\WINNT="Windows XP Professional"
/fastdetect
```

Editing the Boot.ini file

1. Click Start, point to Programs, point to Accessories, and then click Notepad.

2. In Notepad, click Open on the File menu.
3. Click the %systemroot% drive in the Look in box, click the Boot.ini file, and then click Open.

Removing an operating system from the menu

1. In Notepad, select the line that contains information about the operating system you want to remove, and then press DELETE. Example of the line to select:

```ini
multi(0)disk(1)rdisk(0)partition(2)\Windows="Windows 98" /fastdetect
```

2. On the File menu, click Save.

Modifying the operating system menu order

1. In Notepad, select the line that needs to be moved, press CTRL+C, press DELETE, click to place the cursor to where the line needs to be placed, and then press CTRL+V.
2. Repeat step 1 as needed for your configuration, and then click Save on the File menu.

Modifying the default operating system

The default represents the operating system that will be loaded if no selection is made before the time-out occurs.

1. In Notepad, modify the following line to reflect the operating system that is to be the default:

```ini
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
```

For example, changing the default from Windows 2000 Server to Microsoft Windows 95

```ini
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
```

would be modified to:

```ini
default=multi(0)disk(0)rdisk(1)partition(2)\Windows
```

2. On the File menu, click Save.

Modifying the time-out

The time-out represents the number of seconds you are allowed to select an operating system from the menu before the default operating system is loaded.

1. In Notepad, edit the following line to reflect the number of seconds needed.timeout=30
2. On the File menu, click Save.

Troubleshooting

- If there's a problem with the file that is being edited, copy the original Boot.ini file that was backed up to the %systemroot% folder.

The Specify Windows Installation File Location and the Specify Windows Service Pack Installation File Location Group Policy objects do not behave as described on the Explain tab

Article • 09/23/2021 • 3 minutes to read

This article describes how to edit the registry to specify the location of the Windows Installation files and the location of the Windows Service Pack Installation files.

Applies to: Windows 10 - all editions
Original KB number: 833615

> **Note**
>
> This article contains information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. For information about how to back up, restore, and edit the registry, click the following article number to view the article in the Microsoft Knowledge Base:
> 256986 Description of the Microsoft Windows Registry

Symptoms

When you view the **Explain** tab in the **Properties** of the **Specify Windows Installation File Location** Group Policy object, the text on the **Explain** tab states as:

Specifies an alternate location for Windows installation files.

To enable this setting, enter the fully qualified path to the new location in the "Windows Setup file path" box.

If you disable this setting or do not configure it, the Windows Service Pack Setup source path will be the location used during the last time Windows Setup was run on the system.

When you view the **Explain** tab in the **Properties** of the **Specify Windows Service Pack Installation File Location** Group Policy object, the text on the **Explain** tab states as:

Specifies an alternate location for Windows Service Pack installation files.

To enable this setting, enter the fully qualified path to the new location in the "Windows Service Pack Setup file path" box.

If you disable this setting or do not configure it, the Windows Setup source path will be the location used during the last time Windows Service Pack Setup was run on the system.

However, if you try to use these Group Policy objects to specify an alternative location for the Windows installation files and the Windows Service Pack installation files, the files are not retrieved from the location that you specify, and you are prompted for the location of the installation media that was originally used.

Cause

This behavior occurs because the information that is provided on these two **Explain** tabs is inaccurate. The settings for the **Specify Windows Installation File Location** and the **Specify Windows Service Pack Installation File Location** Group Policy objects apply only to Windows File Protection. These settings do not apply to items that use the Setup API to install.

Resolution

To resolve this problem, edit the registry to specify the location of the Windows installation files and the location of the Windows Service Pack installation files. To do it, follow these steps.

> ⚠ **Warning**
>
> If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

1. Click **Start**, click **Run**, type regedit in the **Open** box, and then click **OK**.
2. Locate the following registry subkey:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Setup`
3. Right-click **SourcePath**, and then click **Modify**.

4. In the **Value data** box, type the path of the Windows installation files, and then click **OK**.
5. Right-click **ServicePackSourcePath**, and then click **Modify**.
6. In the **Value data** box, type the path of the Windows Service Pack installation files, and then click **OK**.
7. Locate the following registry subkey:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion`
8. Right-click **SourcePath**, and then click **Modify**.
9. In the **Value data** box, type the path of the Windows installation files, and then click **OK**.

Status

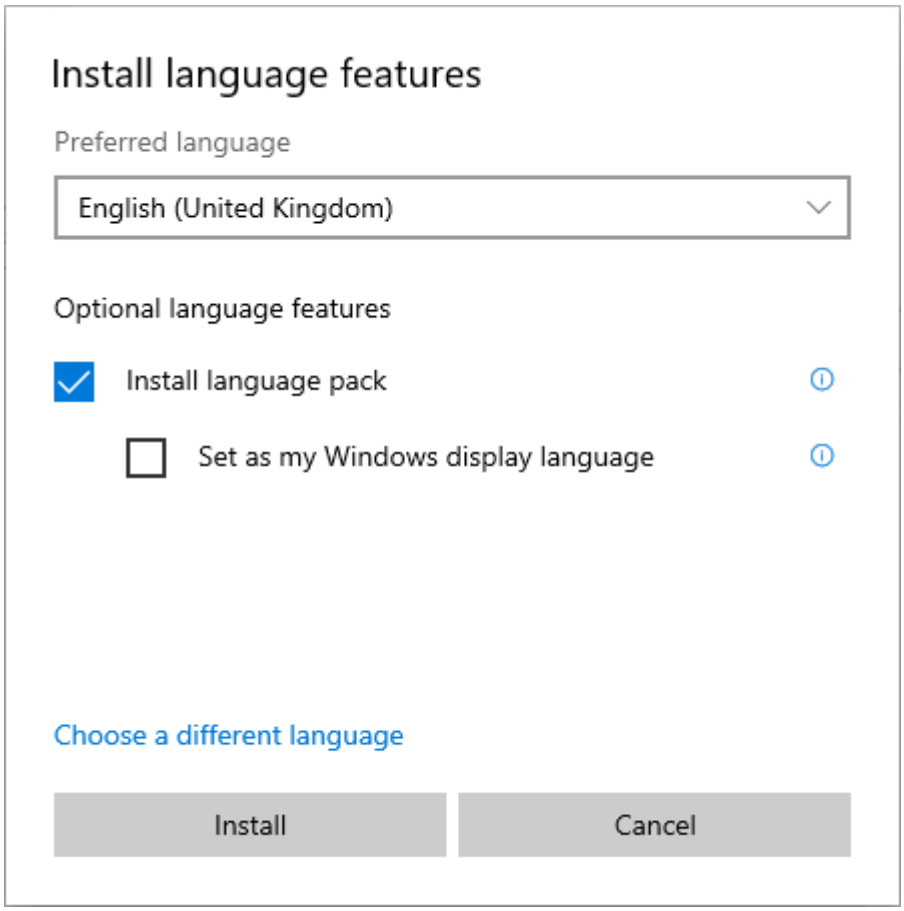
Microsoft has confirmed that it is a problem in the Microsoft products that are listed in the "Applies to" section of this article.

Language features aren't displayed in Windows 10

Article • 12/06/2021 • 2 minutes to read

Applies to: Windows 10, version 1809
Original KB number: 4507173

In versions of Windows prior to Windows 10, version 1809, language features such as **Speech** and **Handwriting** are visible to standard users. When standard users try to add a language feature, a User Account Control (UAC) is prompted and admin credentials are required. Starting from version 1809, language features aren't displayed to standard users as shown here:



Use the Deployment Image Servicing and Management (DISM) cmdlet to include these features in a Windows image.

Language packs are no longer available after upgrading

Article • 11/26/2021 • 2 minutes to read

This article discusses that previously installed language packs are no longer available after you upgrade from Windows 8 to Windows 8.1.

Applies to: Windows 10 - all editions
Original KB number: 2910256

Symptoms

After you upgrade from Windows 8 to Windows 8.1, language packs that were installed before the upgrade are no longer available. You can still switch to the keyboard layout of the languages that were installed before the upgrade. However, the only available display language is the base language version of the Windows installation. In some cases, you cannot reinstall the language packs or change the display language of Windows.

Cause

This behavior is by design. Language packs are not upgraded as part of the operating system upgrade. This issue occurs because Windows 8 and Windows 8.1 each have version-specific language packs. When you upgrade Windows 8 to Windows 8.1, the operating system reverts to its base language version. After the upgrade is finished, you have to reinstall any language packs that you require.

It is also possible that the Advanced language options are set to cause Windows to use a display language that is not yet installed after the upgrade. It causes a condition that prevents you from being able to change the display language or download language packs.

Resolution

Follow Resolution 1 to install the language packs. If you have issues downloading or installing language packs, go to Resolution 2.

Resolution 1: Install the language packs

The instructions for installing language packs can be found in the following Microsoft Knowledge Base article:
Language packs are available for Windows 8 and for Windows RT

Download a language pack from the Windows website

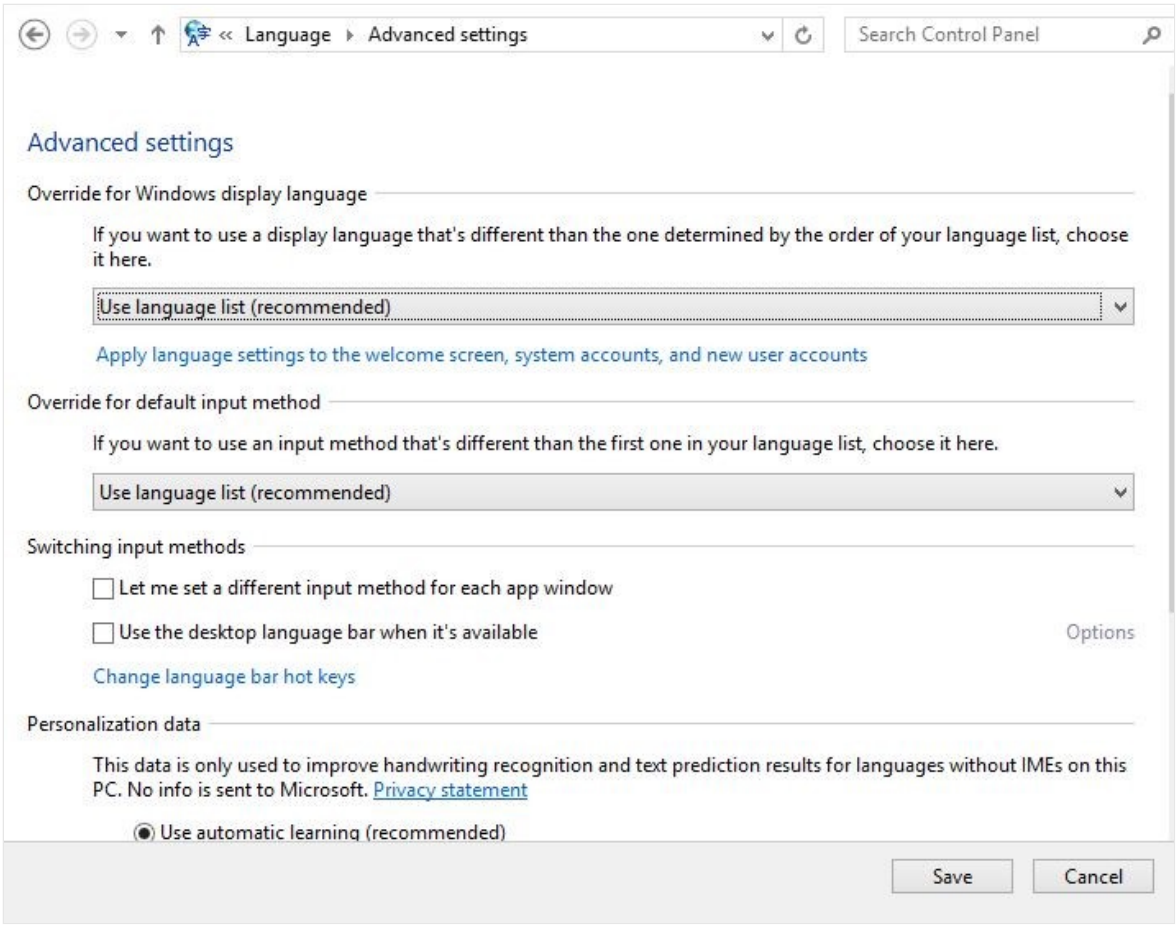
Language packs are sometimes unavailable, and you cannot download them in Control Panel. If you experience this issue, try to find and download the language pack that you want on the following Windows website:
Language packs
If you cannot download a management pack, go to Resolution 2.

Resolution 2: Change settings that may block installation

There are advanced language settings that may block the download of language packs. To revert these settings to their defaults values so that you can download language packs, follow these steps:

1. Open Control Panel. To do it, type Control Panel in the **Search** box, and then tap or click **Control Panel** in the search results list.
2. Tap or click **Clock, Language and Region**. (If you are viewing Control Panel in icon display, select **Language**, and then go to step 4.)
3. Tap or click **Language**.
4. Tap or click **Advanced settings**.
5. Examine the **Override for Windows display language** and **Override for default input method** lists. Make sure that the **Use language list (recommended)** option is selected for both lists (see Figure 1). Then, tap or click **Save**.

   Figure 1: Advanced settings

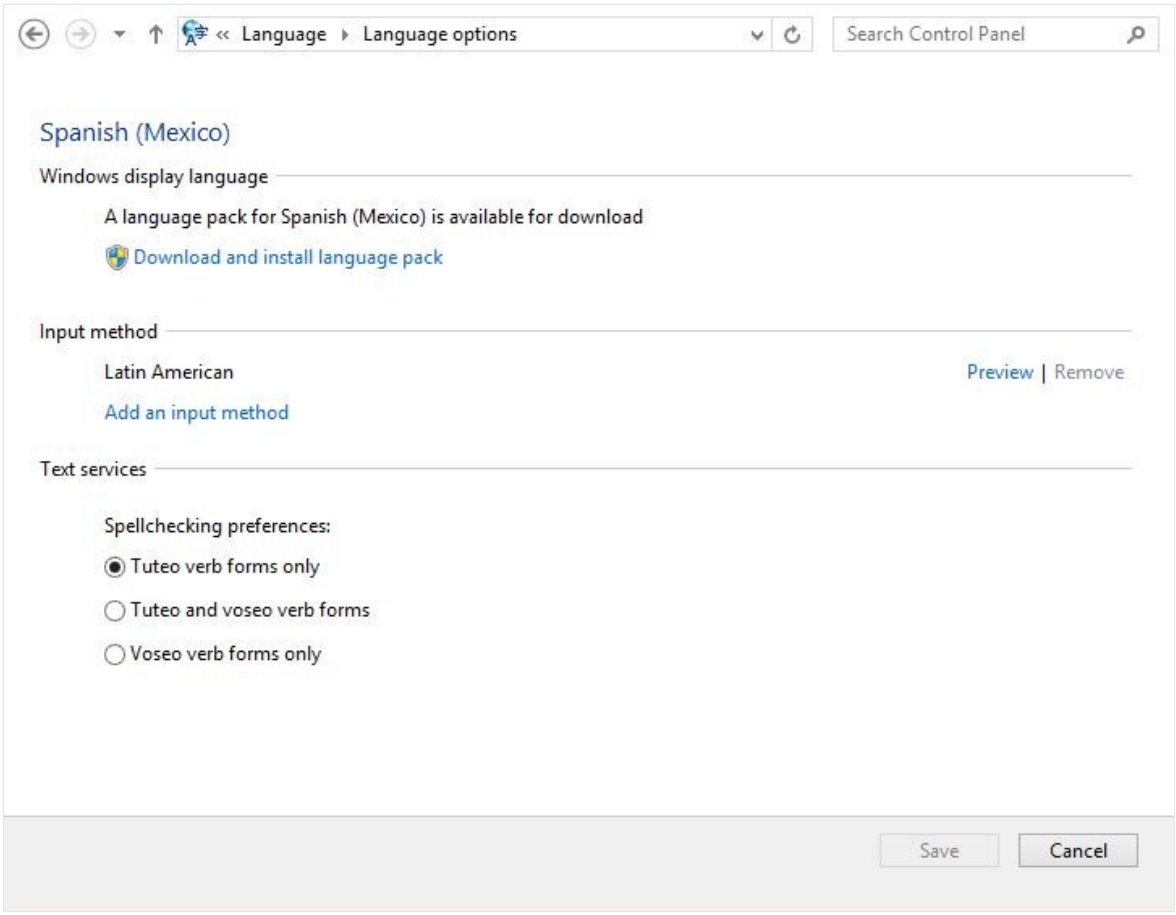


6. After you save the settings, you are returned to the standard language settings. In the list of previously installed languages, click **Options** next to the language you want to install.

7. Click the download link to install the language pack (see Figure 2).

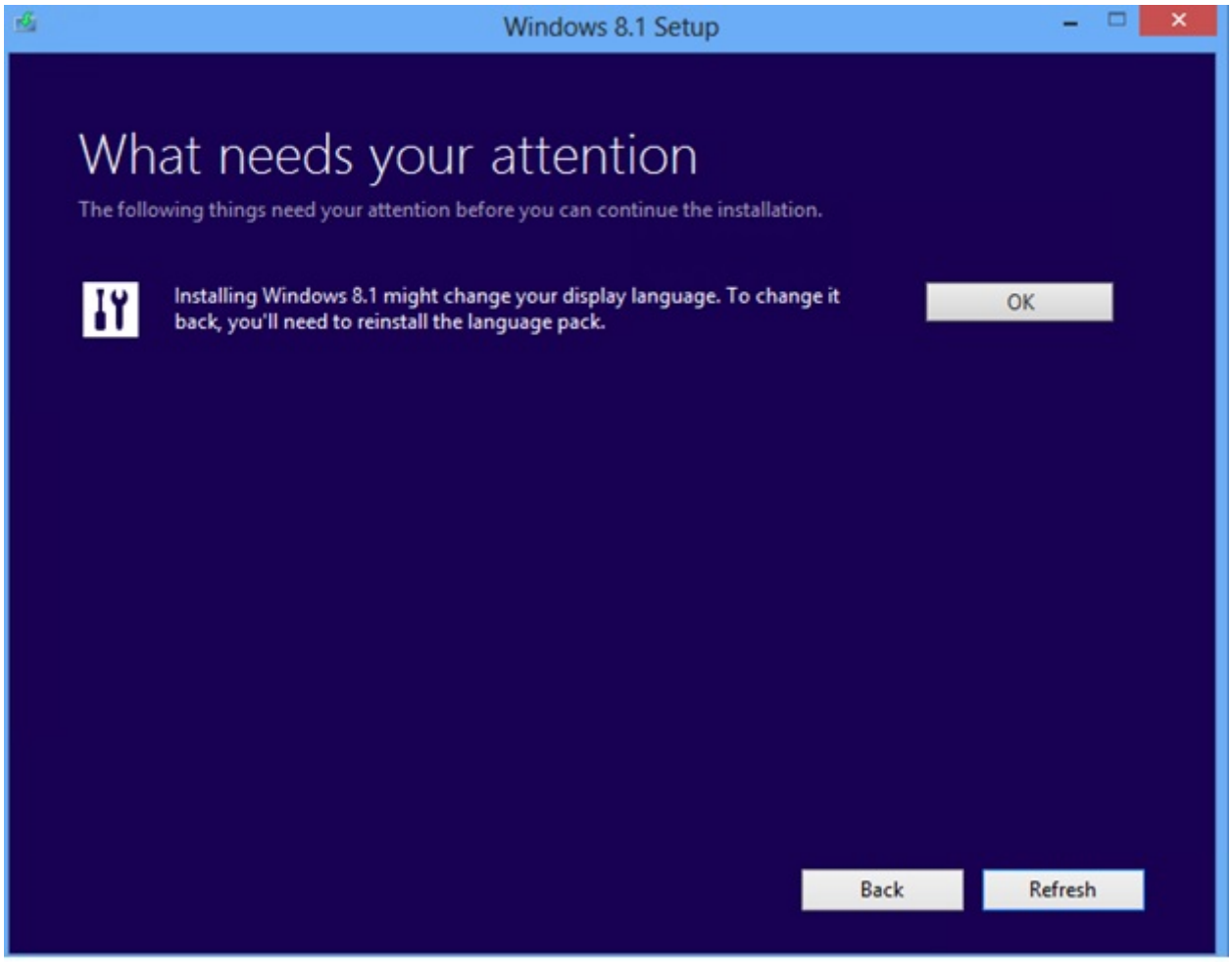
> ⓘ **Note**
>
> After the installation is finished, you are prompted to restart the computer.

Figure 2: Start the download



More information

During the upgrade from Windows 8 to Windows 8.1, Windows Setup detects whether the display language is the localized language of the operating system. It then displays the following message window to indicate that you might have to reinstall any language packs that were previously installed.


Windows 8.1 Setup
What needs your attention
The following things need your attention before you can continue the installation.
Installing Windows 8.1 might change your display language. To change it back, you'll need to reinstall the language pack.
OK
Back
Refresh

MiracastView package cause sysprep error after you upgrade a computer to Windows 10 Version 1709

Article • 11/26/2021 • 2 minutes to read

This article provides workarounds to an issue in which sysprep fails with an error after you upgrade a computer to Windows 10 Version 1709.

Applies to: Windows 10, version 1709
Original KB number: 4057974

Symptoms

Consider the following scenario:

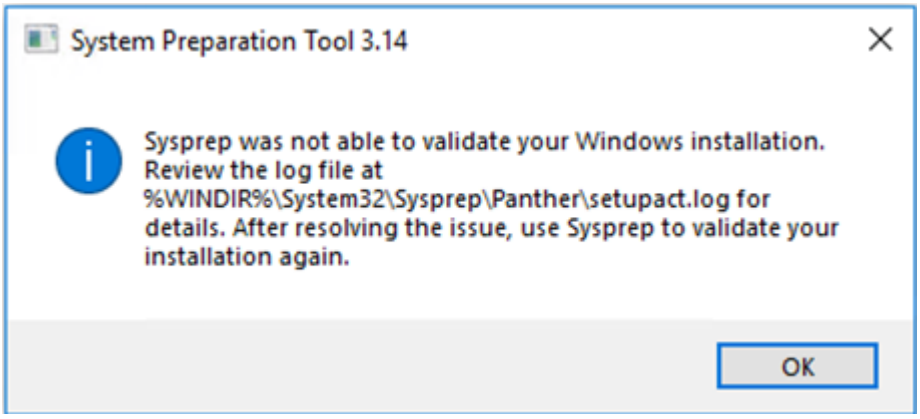
- On a Windows 10 Version 1703 based computer, MiracastView is a built-in app and is installed by default.
- You upgrade the computer to Windows 10 Version 1709.
- You open a Command Prompt window with administrator permission and run the following command:

```
Console

cd %windir%\System32\Sysprep
sysprep.exe /generalize /oobe /reboot
```

In this scenario, the sysprep command fails. You receive an error message that resembles the following:

> Sysprep was not able to validate your Windows installation. Review the log file at %WINDIR%\System32\Sysprep\Panther\setupact.log for details. After resolving the issue, use Sysprep to validate your installation again.

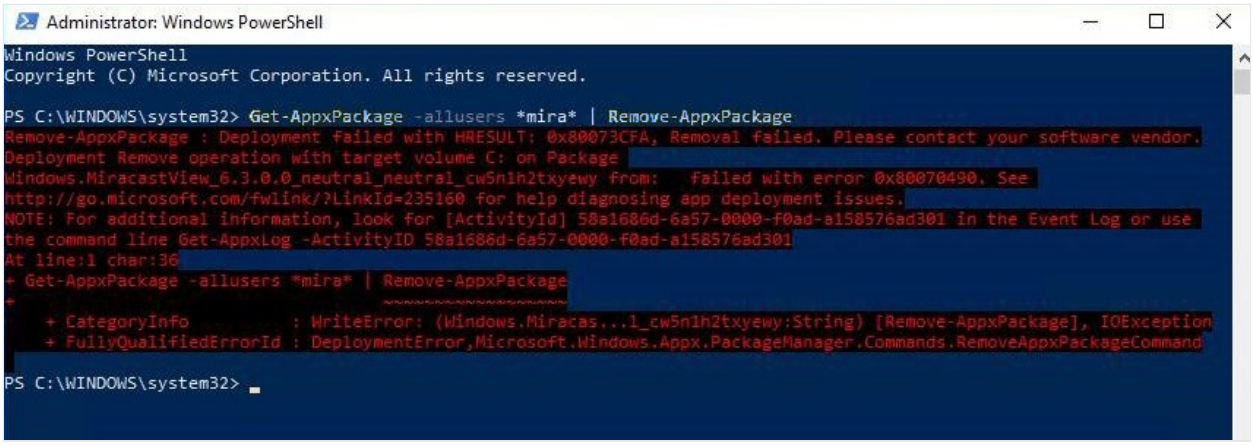


Additionally, the setupact log contains error messages that resemble the following:

> Date/Time, Error SYSPRP Package **Windows.MiracastView_6.3.0.0_neutral_neutral_cw5n1h2txyewy was installed for a user, but not provisioned for all users**. This package will not function properly in the sysprep image.
> Date/Time, Error SYSPRP Failed to remove apps for the current user: 0x80073cf2.
> Date/Time, Error SYSPRP Exit code of RemoveAllApps thread was 0x3cf2.
> Date/Time, Error SYSPRP ActionPlatform::LaunchModule: Failure occurred while executing 'SysprepGeneralizeValidate' from C:\Windows\System32\AppxSysprep.dll; dwRet = 0x3cf2
> Date/Time, Error SYSPRP SysprepSession::Validate: Error in validating actions from C:\Windows\System32\Sysprep\ActionFiles\Generalize.xml; dwRet = 0x3cf2R

When you use the Remove-AppxPackage PowerShell command to remove MiracastView, the command does not work, and you receive the following error message:

> Deployment Remove operation with target volume C: on Package Windows.MiracastView_6.3.0.0_neutral_neutral_cw5n1h2txyewy from: failed with error 0x80070490.
> See `http://go.microsoft.com/fwlink/?LinkId=235160` for help diagnosing app deployment issues.



Cause

This issue occurs due to a bug in the way setup migrated the **Windows.MiracastView_6.3.0.0_neutral_neutral_cw5n1h2txyewy** package during the upgrade. This package will not function properly in the generalized image.

Workaround

To work around this issue, use either of the following methods.

Method 1

On the Windows 10 Version 1709 computer, copy Windows.MiracastView_6.3.0.0_neutral_neutral_cw5n1h2txyewy.xml from C:\Windows.old\ProgramData\Microsoft\Windows\AppRepository\ to C:\ProgramData\Microsoft\Windows\AppRepository.

Method 2

Copy the C:\Windows\MiracastView folder from a Windows 10 Version 1703 computer to the Windows 10 Version 1709 computer. Then, restart the computer to let Windows finish uninstalling MiracastView.

Network provider settings are removed during an in-place upgrade to Windows 10

Article • 12/06/2021 • 2 minutes to read

This article provides workarounds to an issue in which network provider settings are removed during an in-place upgrade to Windows 10.

Applies to: Windows 10, version 1809, Windows 10, version 1709, Windows 10, version 1703, Windows 10, version 1607
Original KB number: 4013822

Symptoms

When you perform an in-place upgrade to Windows 10, version 1809, version 1709, version 1703, or version 1607, the third-party network provider settings are removed from the computer.

Cause

This is a known issue in the Windows 10 upgrade process. After the upgrade, the Provider list (`HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider`) is reset, and the third-party provider registry settings (under `HKLM\System\CurrentControlSet\Services\`) are removed.

Workaround

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, go to the following Microsoft Knowledge Base article:
> 322756 How to back up and restore the registry in Windows

To work around this issue, use one of the following methods.

Method 1

1. Before you upgrade, manually back up the contents of the Provider list at `HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider` and the respective third-party provider settings (under `HKLM\System\CurrentControlSet\Services\`).
2. Run the upgrade.
3. After the upgrade is completed, restore the registry settings that were backed up in step 1.

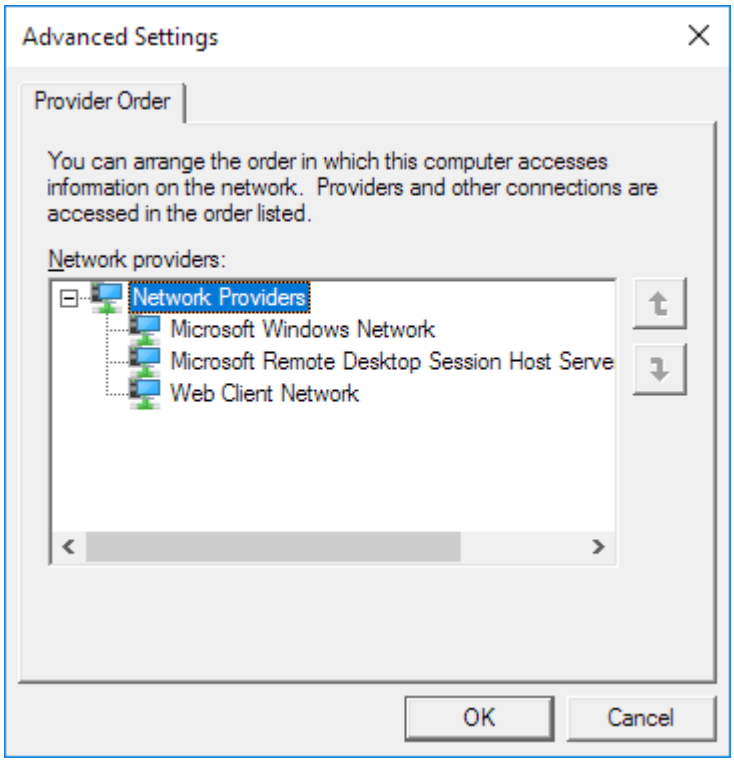
Method 2

If you are experiencing issues that affect the third-party network provider settings after you upgrade, manually restore the registry keys that were deleted by the installer.

More information

To verify the network providers list, follow these steps:

1. Open the **Run** box. To do this, press the Windows logo key ( )+R.
2. Type *ncpa.cpl*, and then press Enter.
3. Press the Alt key to open the menu bar.
4. Select **Advanced**, and then click **Advanced Settings**.



This third-party network providers list is stored in the following registry location:

`HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order\ProviderOrder`

Default value: RDPNP,LanmanWorkstation,webclient

`HKLM\System\CurrentControlSet\Control\NetworkProvider\HwOrder\ProviderOrder`

Default value: RDPNP,LanmanWorkstation,webclient

> ⓘ **Note**
>
> Each string value has its own settings under `HKLM\System\CurrentControlSet\Services`.
> For example, the following are the default network providers:
>
> - `HKLM\System\CurrentControlSet\Services\RDPNP\NetworkProvider`
> - `HKLM\System\CurrentControlSet\Services\LanmanWorkstation\NetworkProvider`
> - `HKLM\System\CurrentControlSet\Services\WebClient\NetworkProvider`
>
> The provider name is removed from the list, and all added registry key are removed.

Multiple operations fail if Windows 8 is improperly identified as a Windows To Go installation

Article • 09/23/2021 • 2 minutes to read

This article discusses issues that occur when Windows 8 is improperly identified as a Windows To Go installation.

Applies to: Windows 8
Original KB number: 2778881

Symptoms

Consider the following scenario:

- You have a computer that is running Windows 8.
- The Windows may report that it's running as a Windows To Go (WTG) installation, while it's not.
- Running or configuring certain Windows components may fail since the OS is reported as Windows to Go. Since these components aren't expected to work and shouldn't work when running Windows To Go installations.

In this scenario, you may notice the following issues:

- Refresh your PC fails reporting:

  Your PC can't be refreshed because it's running Windows To Go

- The Windows To Go control panel reports:

  Can't change startup options when you're in a Windows To Go Workspace

- Microsoft Store fails with error

  Microsoft Store isn't available on Windows To Go Workspaces

Cause

Certain functionality may be blocked from working on Windows To Go Installations as the user experience may not work as desired or expected.

Resolution

To resolve this problem, change the PortableOperatingSystem registry by editing the Windows registry.

> **Note**
>
> This section contains information about how to modify the registry. Make sure that you back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base: 322756 How to back up and restore the registry in Windows

> **Note**
>
> The below mentioned steps should only be followed on machines that aren't running as Windows To Go installations.

To check if the installation is running WTG, Open the Disk Management (diskmgmt.msc) and ensure the Hard Drive the OS is installed to isn't seen as a Removable Drive, which may indicate to the OS that it's running in a Windows To Go scenario.

Prerequisites

Install the following update and then perform the steps mentioned below:

2795944 Windows 8 and Windows Server 2012 cumulative update: February 2013

To change the PortableOperatingSystem registry, follow these steps:

1. Open **Registry editor** (regedit.exe)
2. **Locate** and then select the following registry subkey:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control`

3. From the right-side pane, double-click on **PortableOperatingSystem** Dword value
4. Change the value data to **0** (The default value is 1)
5. Close the registry editor

6. Restart the computer.

You can also use the command-line option to make the change. Run the below command from an elevated command prompt:

Console

```
reg add HKLM\SYSTEM\CurrentControlSet\Control /v PortableOperatingSystem /t
REG_DWORD /d 0
```

Windows 10 Remote Server Admin Tools is uninstalled during in-place upgrade

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution to an issue in which Windows 10 Remote Server Admin Tools (RSAT) is uninstalled during an in-place upgrade.

Applies to: Windows 10 - all editions
Original KB number: 4090941

Symptom

When you perform an in-place upgrade of a Windows 10 installation that has Remote Server Admin Tools (RSAT) installed, RSAT is uninstalled.

Cause

This is by design. RSAT is always uninstalled during in-place upgrades.

Resolution

After the in-place upgrade of Windows 10, reinstall RSAT.

A fatal error occurred while trying to Sysprep the machine error when running Sysprep /generalize

Article • 09/23/2021 • 2 minutes to read

This article solves the issue that you can't run the System Preparation Tool (Sysprep) in Windows 7 by using the `/generalize` option.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 929828

Symptoms

When you try to run the Sysprep in Windows 7, and you use the `/generalize` option, you may receive this error message:

> A fatal error occurred while trying to Sysprep the machine.

The Setuperr.log file may contain lines that resemble the following:

Output

```
Error [0x0f0082] SYSPRP LaunchDll: Failure occurred while executing
'C:\Windows\System32\slc.dll, SLReArmWindows', returned error code
-1073425657
Error [0x0f0070] SYSPRP RunExternalDlls: An error occurred while running
registry sysprep DLLs, halting sysprep execution. dwRet = -1073425657
Error [0x0f00a8] SYSPRP WinMain: Hit failure while processing sysprep
generalize providers; hr = 0xc004d307
```

> ⓘ **Note**
>
> The Setuperr.log file is located in the *\Windows\System32\Sysprep\Panther* folder.

Cause

This error may occur if the Windows Software Licensing Rearm program has run more than three times in a single Windows image.

Resolution

To resolve this issue, you must rebuild the Windows image.

Workaround

To work around this issue, use the <SkipRearm> setting in an XML answer file (Unattend.xml) to skip the Rearm process when you build the Windows image.

The following text is an example of an XML answer file for Windows 7:

XML

```
<settings pass="generalize">
    <component name="Microsoft-Windows-Security-SPP"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <SkipRearm>1</SkipRearm>
    </component>
</settings>
```

> **Note**
>
> You must make sure that the <SkipRearm> setting is removed from the final unattended file that is used to deploy computers in a production environment. If <SkipRearm> is not removed from the unattended file that is used to deploy computers in a production environment, the KMS current client count does not increase for new clients that are added to the network.

For more information about the `skipRearm` tag of Microsoft-Windows-Security-Licensing-SLC component, see SkipRearm.

For more information about `skipRearm` tag of Microsoft-Windows-Security-SPP component, see Microsoft-Windows-Security-SPP.

More information

The Windows Software Licensing Rearm program restores the Windows system to the original licensing state. All licensing and registry data related to activation is either removed or reset. Also, any grace period timers are reset.

To run the Rearm process in Windows 7, use one of the following methods:

- Run `Sysprep /generalize` on the computers that are used to build the custom Windows image.
- Run the Slmgr.vbs script in an elevated Command Prompt window. For example, run `cscript c:\windows\system32\slmgr.vbs -rearm`.

> **Note**
>
> Administrative credentials are required to run the Rearm process. The Rearm process can be run a maximum of three times in a Windows image.

Sysprep and Capture task sequence fails when it tries to capture Windows images

Article • 09/23/2021 • 3 minutes to read

This article provides a workaround for an issue where the Sysprep and Capture task sequence fails when it tries to capture Windows images.

Applies to: Windows 10 - all editions
Original KB number: 2797676

Symptoms

The issue affects the Sysprep and captures TS in the following products:

- Microsoft Deployment 2012 Update 1
- Microsoft Deployment Toolkit 2013

The Sysprep and Capture task sequence fails when it tries to capture a Windows image that was installed from a media. Additionally, you may receive the following errors:

> Deployment Summary
>
> Failure Operating system deployment did not complete successfully.
> Review the log files to determine the cause of the problem.
> During the deployment process, 14 errors and 0 warning were reported.
>
> Details ...
> ZTI ERROR - Unhandled error returned by LTIApply: Not found (-2147217406 0x80041002)
> Litetouch deployment failed, Return Code = -2147467259 0x80004005
> Failed to run the action: Apply Windows PE.
> Not found (Error: 80041002; Source: WMI)
> The execution of the group (Capture Image) has failed and the execution has been aborted.
> An action failed.
> Operation aborted (Error: 80004004; Source: Windows)
> Failed to run the last action: Apply Windows PE. Execution of task sequence failed.
> Not found (Error: 80041002; Source: WMI)
> Task Sequence Engine failed! Code: enExecutionFail

> Task sequence execution failed with error code 80004005
> Error Task Sequence Manaqer failed to execute task sequence. Code 0x80004005

Also, when you check the BDD.log file, you may notice that the following errors are logged:

> <![LOG[Taking ownership of C:\boot]LOG]!><time="<time>" date="<date>" component="LTIApply" context="" type="1" thread="" file="LTIApply">
> <![LOG[About to run command: takeown.exe /F "C:\boot" /R /A /D Y]LOG]!><time="<time>" date="<date>" component="LTIApply" context="" type="1" thread="" file="LTIApply">
> <![LOG[Command has been started (process ID 2748)]LOG]!><time="<time>" date="<date>" component="LTIApply" context="" type="1" thread="" file="LTIApply">
> <![LOG[Return code from command = 1]LOG]!><time="<time>" date="<date>" component="LTIApply" context="" type="1" thread="" file="LTIApply">
> <![LOG[ResetFolder: TakeOwn for C:\boot, RC = 1]LOG]!><time="<time>" date="<date>" component="LTIApply" context="" type="1" thread="" file="LTIApply">
> <![LOG[ZTI ERROR - Unhandled error returned by LTIApply: Not found (-2147217406 0x80041002)]LOG]!><time="<time>" date="<date>" component="LTIApply" context="" type="3" thread="" file="LTIApply">
> <![LOG[Event 41002 sent: ZTI ERROR - Unhandled error returned by LTIApply: Not found (-2147217406 0x80041002)]LOG]!><time="<time>" date="<date>" component="LTIApply" context="" type="1" thread="" file="LTIApply">

Cause

This problem occurs because the LTIApply.wsf script fails to check for the existence of the boot folder on the system partition before the script runs the `takeown.exe` command to change ownership on the folder. The `takeown.exe` command fails with a "Not Found" error if the boot folder doesn't exist. This causes the Sysprep and Capture task sequence to fail.

Workaround

To work around this problem, edit the following files:

- %DeployRoot%\Scripts\LTIApply.wsf

> ⓘ **Note**

%DeployRoot% is the path that you specified when the deployment share was created.

- C:\Program files\Microsoft Deployment Toolkit\Templates\Distribution\Scripts\LTIApply.wsf

Locate the "Copy bootmgr" section in LTIApply.wsf, and then add the following code above the existing code under the "Copy bootmgr" section:

Visual Basic Script

```
If not oFSO.FolderExists(sBootDrive & "\Boot") then
 oFSO.CreateFolder(sBootDrive & "\Boot")
End if
```

More information

This issue doesn't occur if you capture a Windows image that was originally deployed by using MDT 2012 Update 1. This is because when Windows is deployed by using MDT, a System Reserved partition is created that has a size of 499 megabytes (MB). There is enough free space in the System Reserved partition to apply the WinPE image that is required for the capture.

If the Windows image that you are trying to capture with the Sysprep and Capture task sequence was originally deployed from a Windows media, the System Reserved partition that is created has a size of 350 MB. And because it already contains the WinRE image, it does not have enough free space for MDT to apply the WinPE image. In this case, the LTIApply script automatically selects the System Partition to apply the WinPE image. As part of this process, the LTIApply script changes ownership on the bootmgr file and the boot folder on the System Partition. The problem occurs because the LTIApply script doesn't check for the existence of the boot folder on the System Partition before it runs the `takeown.exe` command to change ownership.

System Restore points are disabled after you upgrade to Windows 10

Article • 12/06/2021 • 2 minutes to read

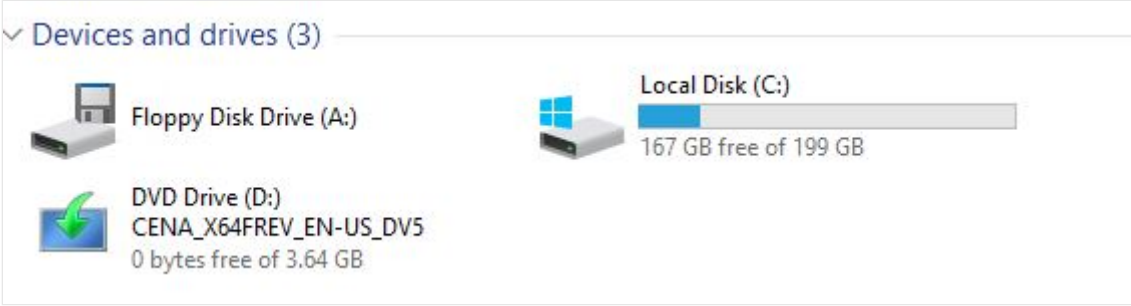
This article discusses an issue where you can't restore the system to an earlier restore point after an upgrade to Windows 10.

Applies to: Windows 10 - all editions
Original KB number: 3209726

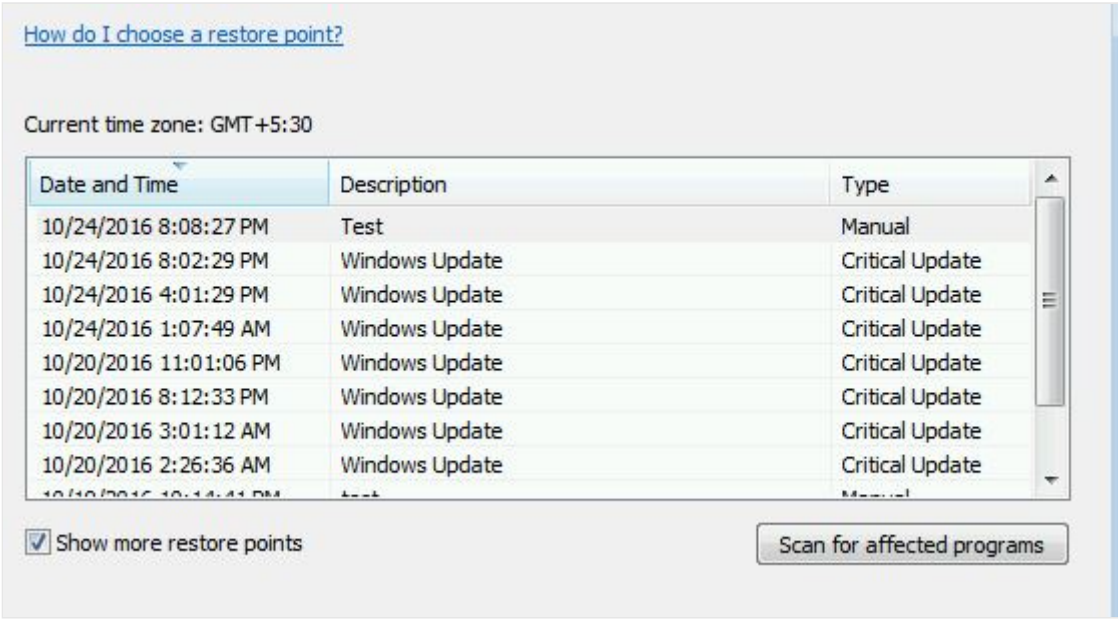
Symptoms

Assume that you have a Windows 7-based system with system restore points set, and the computer is upgraded to Windows 10. When you try to restore the system to an earlier restore point after the upgrade, you discover that you can't do that. The option is disabled.

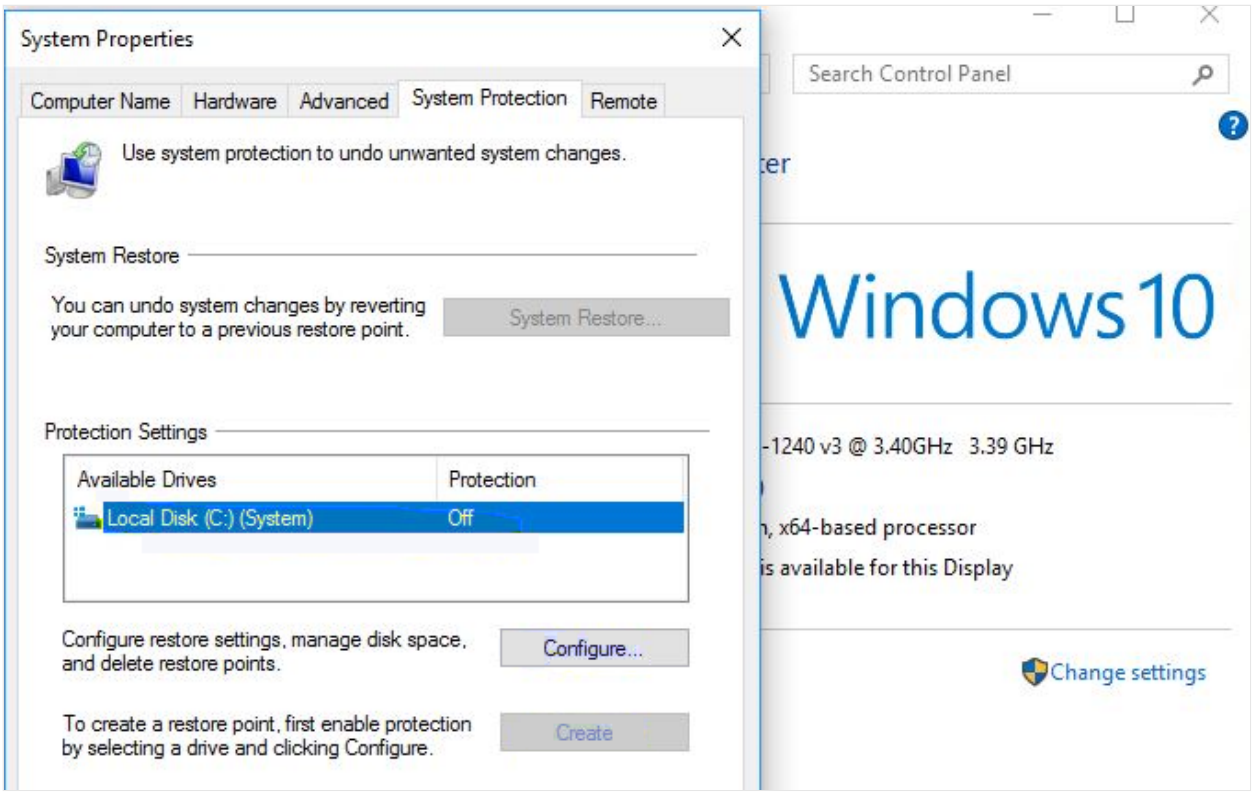
Windows 7 Disk Size:



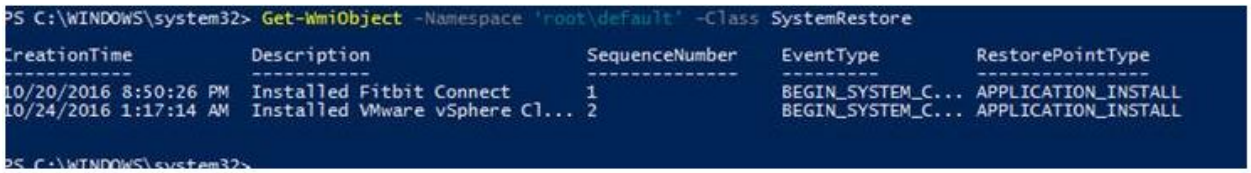
Restore points on Windows 7:



Restore points after you upgrade to Windows 10:



Querying the System Restore via PowerShell:



Cause

This issue occurs because system restore points don't persist after a Windows upgrade. This behavior is by design.

More information

By default, System Restore should be disabled after an upgrade regardless of its earlier setting, and all the older Restore Points will be deleted from System Restore. However, on an MSI or Windows Update installation, if the size of the operating system disk is greater than 128 gigabytes (GB), a restore point is automatically created without the user enabling System Restore (as if System Restore were already enabled). Similarly, if the disk size is less than 128 GB, no restore point is created until System Restore is manually enabled.

You can verify this yourself by checking for a restore point after a .msi or Windows Update installation on a computer that has a disk size of greater than 128 GB.

For more information about System Restore, see How to Use System Restore in Windows 7, 8, and 10 and Backup and restore in Windows 10.

How to use the Ocsetup.exe tool to install or to remove Windows optional components in Windows Vista

Article • 09/23/2021 • 3 minutes to read

This article describes how to use the Windows optional component setup tool (Ocsetup.exe) to install or to remove Windows optional components.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 936209

Summary

Windows optional components are parts of the Windows operating system that can be individually added, removed, enabled, or disabled. You can use the Ocsetup.exe tool at the command prompt to install or to remove Windows Vista optional components. You must have administrative credentials to run the Ocsetup.exe tool.

Use Ocsetup.exe to install Windows optional components

1. Click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.
2. At the command prompt, type the following command, and then press ENTER:
   `start /w ocsetup <Optional component name>`

> **Note**
>
> - In step 2, **Optional component name** specifies the name of the Windows optional component. The optional component name is case-sensitive. For example, if you want to install the DHCP Server role, type `start /w ocsetup DHCPServerCore`, and then press ENTER.
> - To determine the correct optional component name for Windows Vista to use with the ocsetup command line, visit the following Web page, and then review the "Command-Line Name" column in the Microsoft-Windows-Foundation-Package Features table: **Windows Vista Packages**

3. Type *exit*, and then press ENTER to close the Command Prompt window.

> **Note**
>
> To display the list of command-line switches that the Ocsetup.exe tool supports, type ocsetup at the command prompt, and then press ENTER.

Use Ocsetup.exe to remove Windows optional components

1. Click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.
2. At the command prompt, type the following command, and then press ENTER:
   `start /w ocsetup <Optional component name> /uninstall`

   > **Note**
   >
   > - In step 2, **Optional component name** specifies the name of the Windows optional component. The optional component name is case-sensitive. For example, if you want to remove the DHCP Server role, type `start /w ocsetup DHCPServerCore/uninstall`, and then press ENTER.
   > - To determine the name of the Windows optional component, click **Start**, type *optionalfeatures* in the **Start Search** box, and then click **optionalfeatures** in the **Programs** list.

3. Type *exit*, and then press ENTER to close the Command Prompt window.

   > **Note**
   >
   > To display the list of command-line switches that the Ocsetup.exe tool supports, type ocsetup at the command prompt, and then press ENTER.

Ocsetup.exe tool functionality

The Ocsetup.exe tool provides functionality that resembles the functionality that the Sysocmgr.exe tool provides in Microsoft Windows XP and in Microsoft Windows Server 2003. In Windows Vista, Windows Defender Software Explorer and Windows Update use

the Ocsetup.exe tool. In Windows Server 2008, Server Manager uses the Ocsetup.exe tool.

The Ocsetup.exe tool is used as a wrapper for Package Manager (Pkgmgr.exe) and for Windows Installer (Msiexec.exe). Ocsetup.exe is a command-line utility that can be used to perform scripted installs and scripted uninstalls of Windows optional components. The Ocsetup.exe tool replaces the Sysocmgr.exe tool that Windows XP and Windows Server 2003 use.

Windows optional components can be MSI-based or component-based. The Ocsetup.exe tool detects the type of optional component that is passed as a parameter. Additionally, the Ocsetup.exe tool calls the correct child process to install or to remove the optional component. If the optional component is MSI-based, the Ocsetup.exe tool calls Msiexec.exe. If the optional component is component-based, the Ocsetup.exe tool calls Pkgmgr.exe. The Ocsetup.exe tool returns back to the caller the exit code that is received from Pkgmgr.exe, from Msiexec.exe, or from the custom bootstrapping application.

For system optional components that are MSI-based, the Ocsetup.exe tool first checks a registry location to determine one of the following:

- If a component uses the generic bootstrapping application (Ocsetup.exe).
- If a component has a special custom-made bootstrapping application that performs install tasks or removal tasks. Based on this determination, the Ocsetup.exe tool passes the task to the custom bootstrapping application, or the Ocsetup.exe tool internally performs generic bootstrapping tasks. The Ocsetup.exe tool performs the following generic tasks:
- Checks the cache directory for updates.
- Passes the MSI package name and the MSI package location to Windows Installer.
- Passes names of one or more .msp files to Windows Installer. The Ocsetup.exe tool also accepts configuration information that is supplied as an unattended file. For more information, see the unattended documentation.

References

For more information about command-line options that are available for Package Manager, visit the following Microsoft Web site: Package Manager Command-Line Options

For more information about Windows Installer, visit the following Microsoft Web site: Windows Installer

Windows Vista, Windows 7, Windows Server 2008 R2, Windows 8.1, and Windows 10 setup log file locations

Article • 03/24/2022 • 4 minutes to read

This article describes where to locate these log files and which log files are most useful for troubleshooting each setup phase of Windows 7, of Windows Server 2008 R2, and of Windows Vista.

Applies to: Windows 10 - all editions, Windows Server 2019, Windows Server 2016
Original KB number: 927521

Introduction

Windows setup log files are in different locations on the hard disk. These locations depend on the setup phase.

Support for Windows Vista without any service packs installed ended on April 13, 2010. To continue receiving security updates for Windows, make sure you're running Windows Vista with Service Pack 2 (SP2). For more information, see Windows XP support has ended.

Down-level phase

The downlevel phase is the Windows setup phase that is running within the previous operating system. The following table lists important log files in this setup phase.

Log file	Description
C:\WINDOWS\setupapi.log	Contains information about device changes, driver changes, and major system changes, such as service pack installations and hotfix installations. This log file is used only by Microsoft Windows XP and earlier versions.
C:$WINDOWS.~BT\Sources\Panther\setupact.log	Contains information about setup actions during the installation.

Log file	Description
C:$WINDOWS.~BT\Sources\Panther\setuperr.log	Contains information about setup errors during the installation.
C:$WINDOWS.~BT\Sources\Panther\miglog.xml	Contains information about the user directory structure. This information includes security identifiers (SIDs).
C:$WINDOWS.~BT\Sources\Panther\PreGatherPnPList.log	Contains information about the initial capture of devices that are on the system during the downlevel phase.

Windows Preinstallation Environment phase

The Windows Preinstallation Environment (Windows PE or WinPE) phase is the Windows setup phase that occurs after the restart at the end of the downlevel phase, or when you start the computer by using the Windows installation media. The following table lists important log files in this setup phase.

Log file	Description
X:$WINDOWS.~BT\Sources\Panther\setupact.log	Contains information about setup actions during the installation.
X:$WINDOWS.~BT\Sources\Panther\setuperr.log	Contains information about setup errors during the installation.
X:$WINDOWS.~BT\Sources\Panther\miglog.xml	Contains information about the user directory structure. This information includes security identifiers (SIDs).
X:$WINDOWS.~BT\Sources\Panther\PreGatherPnPList.log	Contains information about the initial capture of devices that are on the system during the downlevel phase.
or	
C:$WINDOWS.~BT\Sources\Panther\setupact.log	Contains information about setup actions during the installation.
C:$WINDOWS.~BT\Sources\Panther\setuperr.log	Contains information about setup errors during the installation.
C:$WINDOWS.~BT\Sources\Panther\miglog.xml	Contains information about the user directory structure. This information includes security identifiers (SIDs).

Log file	Description
C:$WINDOWS.~BT\Sources\Panther\PreGatherPnPList.log	Contains information about the initial capture of devices that are on the system during the downlevel phase.

> ⓘ Note
>
> You may also see a log file in the `X:\WINDOWS` directory. The Setupact.log file in this directory contains information about the progress of the initial options that are selected on the Windows installation screen. The Windows installation screen appears when you start the computer by using the Windows installation media. After you select **Install now** from the Windows installation screen, the Setup.exe file starts, and this log file is no longer used.

Online configuration phase

The online configuration phase (the first boot phase) starts when you receive the following message:

> Please wait a moment while Windows prepares to start for the first time.

During this phase, basic hardware support is installed. If it's an upgrade installation, data and programs are also migrated. The following table lists important log files in this setup phase.

Log file	Description
C:\WINDOWS\PANTHER\setupact.log	Contains information about setup actions during the installation.
C:\WINDOWS\PANTHER\setuperr.log	Contains information about setup errors during the installation.
C:\WINDOWS\PANTHER\miglog.xml	Contains information about the user directory structure. This information includes security identifiers (SIDs).
C:\WINDOWS\INF\setupapi.dev.log	Contains information about Plug and Play devices and driver installation.
C:\WINDOWS\INF\setupapi.app.log	Contains information about application installation.

Log file	Description
C:\WINDOWS\Panther\PostGatherPnPList.log	Contains information about the capture of devices that are on the system after the online configuration phase.
C:\WINDOWS\Panther\PreGatherPnPList.log	Contains information about the initial capture of devices that are on the system during the downlevel phase.

Windows Welcome phase

The Windows Welcome phase includes the following options and events:

- It provides the options to create user accounts.
- It provides the option to specify a name for the computer.
- The Windows System Assessment Tool (Winsat.exe) finishes performance testing to determine the Windows Experience Index rating.

The Windows Welcome phase is the final setup phase before a user signs in. The following table lists important log files in this setup phase.

Log file	Description
C:\WINDOWS\PANTHER\setupact.log	Contains information about setup actions during the installation.
C:\WINDOWS\PANTHER\setuperr.log	Contains information about setup errors during the installation.
C:\WINDOWS\PANTHER\miglog.xml	Contains information about the user directory structure. This information includes security identifiers (SIDs).
C:\WINDOWS\INF\setupapi.dev.log	Contains information about Plug and Play devices and driver installation.
C:\WINDOWS\INF\setupapi.app.log	Contains information about application installation.
C:\WINDOWS\Panther\PostGatherPnPList.log	Contains information about the capture of devices that are on the system after the online configuration phase.
C:\WINDOWS\Panther\PreGatherPnPList.log	Contains information about the initial capture of devices that are on the system during the downlevel phase.

Log file	Description
C:\WINDOWS\Performance\Winsat\winsat.log	Contains information about the Windows System Assessment Tool performance testing results.

Rollback phase

If a Windows upgrade installation fails, and you've successfully rolled back the installation to the previous operating system desktop, there are several log files that you can use for troubleshooting. The following table lists important log files in this phase.

Log file	Description
C:$WINDOWS.~BT\Sources\Panther\setupact.log	Contains information about setup actions during the installation.
C:$WINDOWS.~BT\Sources\Panther\miglog.xml	Contains information about the user directory structure. This information includes security identifiers (SIDs).
C:$WINDOWS.~BT\Sources\Panther\setupapi\setupapi.dev.log	Contains information about Plug and Play devices and driver installation.
C:$WINDOWS.~BT\Sources\Panther\setupapi\setupapi.app.log	Contains information about application installation.
C:$WINDOWS.~BT\Sources\Panther\PreGatherPnPList.log	Contains information about the initial capture of devices that are on the system during the downlevel phase.
C:$WINDOWS.~BT\Sources\Panther\PostGatherPnPList.log	Contains information about the capture of devices that are on the system after the online configuration phase.

Error message: Windows SIM was unable to generate a catalog or Parameter count mismatch

Article • 09/23/2021 • 2 minutes to read

This article helps fix errors that occur when generating a catalog (.clg) in Windows System Image Manager (WSIM).

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2524737

Symptoms

When generating a catalog (.clg) in Windows System Image Manager (WSIM) or clicking Edit Unattend.xml in Microsoft Deployment Toolkit (MDT) and trying to generate a catalog file, it may take extended period of time before producing the error message and you may receive the following error messages:

> Windows SIM was unable to generate a catalog. For troubleshooting assistance, see the topic: 'Windows System Image Manager Technical Reference' in the Windows OPK or Windows AIK User's Guide. System.InvalidOperationException: The operation failed to complete.

or

> Windows System Image Manager execution failed. System.Reflection.TargetParameterCountException: Parameter count mismatch.

or

> Performing operation "generate" on Target "Catalog". The operation failed to complete

Cause

Windows System Image manager has the following default behavior for generating catalog files:

x86 Windows System Image Manager

Can create catalogs for x86, x64, and Itanium-based Windows images.

x64 Windows System Image Manager

Can create catalogs only for x64 Windows images.

Itanium-based Windows System Image Manager

Can create catalogs only for Itanium-based Windows images

Resolution

Generate the catalog file on a supported platform. For Microsoft Deployment Toolkit, it's possible to mount the DeploymentShare from another computer with MDT and the AIK installed with the proper architecture to generate the catalog then it can be accessed by the original MDT server.

More information

This is by design. For more information, see Understanding Windows Image Files and Catalog Files

Windows 7 Upgrade Advisor tool failed to run with error message "Windows 7 Upgrade Advisor was unable to reach the Microsoft server for compatibility information. Check your internet connection and try again later."

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an error that occurs when you run the Windows 7 Upgrade Advisor tool on a system.

Applies to: Windows 7 Service Pack 1
Original KB number: 2448270

Symptoms

When you run the Windows 7 Upgrade Advisor tool on a system that must use a proxy to access the internet, you receive the error:

> Windows 7 Upgrade Advisor was unable to reach the Microsoft server for compatibility information. Check your internet connection and try again later.

Cause

Windows 7 Upgrade Advisor tries to reach the Microsoft server to get the compatibility information. The error is shown since Windows 7 Upgrade Advisor doesn't support proxy authentication.

In the error log (%temp%\WuaDiagnostics.log), you receive the error like following one:

> [7/23/2010 12:04:41 PM] Exception: The request failed with HTTP status 407: Proxy Authentication Required

Resolution

On the proxy, create an anonymous access rule specific to the destinations FQDN (fully qualified domain name)'s used by the Windows 7 Upgrade Advisor, for example, you may create the following rules:

> Action: Allow
> Protocols: HTTP, HTTPS
> From/Listener: Internal
> To: Domain Name Set
> aeos.microsoft.com
> aestats.microsoft.com
> crl.microsoft.com
> download.microsoft.com
> go.microsoft.com
>
> Condition: All Users

WinRE can't be built after you deploy a Windows 8.1 image

Article • 09/23/2021 • 3 minutes to read

This article provides a solution to an issue in which you can't deploy a Windows 8.1-based image to a UEFI computer when the image was captured from a non-UEFI computer.

Applies to: Windows 8.1
Original KB number: 2952359

Symptoms

Assume that you have a Windows 8.1 image that was captured from a non-UEFI computer. After you deploy the image to a UEFI computer, the Windows Recovery Environment (WinRE) can't be built on the UEFI computer.

When this issue occurs, messages that resemble the following are logged in the setupact.log file. The messages indicate that the setup process can't find the staged WinRE image, and that the WinRE can't be built:

> <DateTime>, Info [setup.exe] WinReInstallOnTargetOS Beginning WinRE installation.
> <DateTime>, Info [setup.exe] winreCheckRegKeyTest hook (S) present or enabled
> <DateTime>, Info [setup.exe] WinReInstallOnTargetOS System setup is in progress.
> <DateTime>, Info [setup.exe] WinReInstallOnTargetOS Checking for downlevel WinRE installation.
> <DateTime>, Info [setup.exe] ReAgentXMLParser::ParseConfigFile (xml file: \Recovery\ReAgentOld.xml) returning 0X3
> <DateTime>, Info [setup.exe] ReAgentConfig::ParseConfigFile returned with 0x3
> <DateTime>, Info [setup.exe] WinReInstallOnTargetOS Getting current WinRE configuration.
> <DateTime>, Info [setup.exe] WinReInstallOnTargetOS Disabling extra ReAgentConfig BCD checks for legacy setup.
> <DateTime>, Info [setup.exe] WinReInstallOnTargetOS No source winre.wim was specified. Checking for a staged winre.wim.
> <DateTime>, Info [setup.exe] WinReInstallOnTargetOS Searching for OEM Winre.wim
> <DateTime>, Info [setup.exe] WinReInstallOnTargetOS Error 0X2 while searching for OEM winre.wim

> <DateTime>, Warning [setup.exe] WinReInstallOnTargetOS (WinRE)WinREInstall() returning FALSE, gle = 0x64E

Cause

This issue occurs because the ImageLocation path tag is set to the \Recovery\WindowsRE value and the WinREStaged state tag is set to 1 in the Reagent.xml file. For more information, go to the more information section.

Resolution

To resolve this issue, use one of the following methods:

- Use the Windows 8.1 image that was captured from a UEFI computer to deploy to a UEFI computer.
- Change the Reagent.xml file that is located in the \Windows\System32\Recovery\Reagent.xml path inside the captured .wim file from non-UEFI computers by making the following changes:
  - Remove the value of the ImageLocation path tag by using "".
  - Set the value of the WinREStaged state tag to 0.

For example, change the XML file as follows:

XML

```
<?xml version='1.0' encoding='utf-8' standalone='yes'?>
<WindowsRE version="2.0">
    <WinreBCD id=""></WinreBCD>
    <WinreLocation path="" id="0" offset="0"></WinreLocation>
    <ImageLocation path="" id="0" offset="0"></ImageLocation>
    <PBRImageLocation path="" id="0" offset="0" index="0">
</PBRImageLocation>
    <PBRCustomImageLocation path="" id="0" offset="0" index="0">
</PBRCustomImageLocation>
    <InstallState state="0"></InstallState>
    <OsInstallAvailable state="0"></OsInstallAvailable>
    <CustomImageAvailable state="0"></CustomImageAvailable>
    <WinREStaged state="0"></WinREStaged>
    <ScheduledOperation state="4"></ScheduledOperation>
    <OperationParam path=""></OperationParam>
    <OsBuildVersion path=""></OsBuildVersion>
    <OemTool state="0"></OemTool>
</WindowsRE>
```

More information

An example of the Reagent.xml file

After you capture the Windows 8.1 image from a non-UEFI computer by using Microsoft Deployment Toolkit (MDT) 2013, the \Windows\System32\Recovery\Reagent.xml file inside the WIM image may resemble the following:

XML

```
<?xml version='1.0' encoding='utf-8'?>
<WindowsRE version="2.0">
    <WinreBCD id="{00000000-0000-0000-0000-000000000000}"/>
    <WinreLocation path="" id="0" offset="0" guid="{00000000-0000-0000-0000-
000000000000}"/>
    <ImageLocation path="\Recovery\WindowsRE" id="4238117423"
offset="1048576" guid="{00000000-0000-0000-0000-000000000000}"/>
    <PBRImageLocation path="" id="0" offset="0" guid="{00000000-0000-0000-
0000-000000000000}" index="0"/>
    <PBRCustomImageLocation path="" id="0" offset="0" guid="{00000000-0000-
0000-0000-000000000000}" index="0"/>
    <InstallState state="0"/>
    <OsInstallAvailable state="0"/>
    <CustomImageAvailable state="0"/>
    <IsAutoRepairOn state="1"/>
    <WinREStaged state="1"/>
    <OperationParam path=""/>
    <OsBuildVersion path="9600.16384.amd64fre.winblue_rtm.130821-1623"/>
    <OemTool state="0"/>
    <IsServer state="0"/>
    <DownlevelWinreLocation path="" id="0" offset="0" guid="{00000000-0000-
0000-0000-000000000000}"/>
    <ScheduledOperation state="4"/>
</WindowsRE>
```

In this file, the WinRE image location is set to path \Recovery\WindowsRE, and WinREStaged is set to 1. These settings only work well when you deploy them on non-UEFI computers. If you use the image together with this xml file to build the OS on a UEFI computer such as Surface Pro or Surface Pro 2, the WinRE environment can't be built. Because of the lack of a WinRE environment, BitLocker can't be enabled.

BitLocker does not work when WinRE is disabled

When WinRE is disabled, you can't enable BitLocker, and you receive an error message that resembles the following:

> This PC doesn't support entering a BitLocker recovery password during startup. Ask your administrator to configure Windows Recovery Environment so that you can use BitLocker.

You can also use the `Reagentc.exe /info` command to receive the WinRE status to confirm whether it's enabled. For example, you receive the following results when you run the command:

Console

```
C:\WINDOWS\system32>Reagentc.exe /info
Windows Recovery Environment (Windows RE) and system reset configuration
Information:

Windows RE status: Enabled
 Windows RE location: \\?
\GLOBALROOT\device\harddisk0\partition1\Recovery\WindowsRE
 Boot Configuration Data (BCD) identifier: ########-####-####-####-
############
 Recovery image location:
 Recovery image index: 0
 Custom image location:
 Custom image index: 0

REAGENTC.EXE: Operation Successful.
```

You can't access an EFI system partition with the Mountvol utility in a WinPE Environment

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue that you can't gain access to the Extensible Firmware Interface (EFI) system partition by using the `mountvol /s` command when you use the Mountvol utility (Mountvol.exe) in a WinPE Environment.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 315943

Symptoms

If you use the Mountvol utility (Mountvol.exe) in a Windows Preinstall Environment (WinPE) on either a Windows XP-based or Windows Server 2003-based computer, you can't gain access to the Extensible Firmware Interface (EFI) system partition by using the `mountvol /s` command. For example, if you try to use the `mountvol x: /s` command, you may receive the following error message:

> The system cannot find the file specified.

Cause

This behavior occurs because the Mountvol utility isn't supported in WinPE environments.

Resolution

To work around this behavior, use the Diskpart utility (Dispart.exe) instead of the Mountvol tool. To use the Diskpart utility:

1. Select **Start**, select **Run**, type diskpart in the **Open** box, and then select **OK**.
2. When the Diskpart utility starts, type select disk **n** at the prompt (where **n** is number for the mapped ESP disk), and then press **ENTER**.
3. Type select partition
   n at the prompt (where **n** is number for the mapped ESP partition), and then press **ENTER**.

4. Type assign letter= **x** at the prompt (where **x** is the drive letter that you want to assign), and then press **ENTER**.

After you follow these steps, you can access an EFI system partition by using the drive letter that you assign to the partition with the Diskpart utility.

Status

This behavior is by design.

USMT common issues

Article • 11/25/2022 • 13 minutes to read

The following sections discuss common issues that you might see when you run the User State Migration Tool (USMT) 10.0 tools. USMT produces log files that describe in further detail any errors that occurred during the migration process. These logs can be used to troubleshoot migration failures.

General guidelines for identifying migration problems

When you encounter a problem or error message during migration, you can use the following general guidelines to help determine the source of the problem:

- Examine the **ScanState**, **LoadState**, and UsmtUtils logs to obtain the exact USMT error messages and Windows® application programming interface (API) error messages. For more information about USMT return codes and error messages, see Return codes. You can obtain more information about any listed **Windows** system error codes by typing in a command prompt window `net.exe helpmsg <error_number>` where <*error_number*> is the error code number generated by the error message. For more information about System Error Codes, see System Error Codes (0-499).

  In most cases, the **ScanState** and **LoadState** logs indicate why a USMT migration is failing. We recommend that you use the `/v:5` option when testing your migration. This verbosity level can be adjusted in a production migration; however, reducing the verbosity level might make it more difficult to diagnose failures that are encountered during production migrations. You can use a verbosity level higher than 5 if you want the log files output to go to a debugger.

  > **Note**
  >
  > Running the **ScanState** and **LoadState** tools with the `/v:5` option creates a detailed log file. Although this option makes the log file large, the extra detail can help you determine where migration errors occurred.

- Use the `/Verify` option with the UsmtUtils tool to determine whether any files in a compressed migration store are corrupted. For more information, see Verify the condition of a compressed migration store.

- Use the `/Extract` option with the UsmtUtils tool to extract files from a compressed migration store. For more information, see Extract files from a compressed USMT migration store.
- Create a progress log using the `/Progress` option to monitor your migration.
- For the source and destination computers, obtain operating system information, and versions of applications such as Internet Explorer and any other relevant programs. Then verify the exact steps that are needed to reproduce the problem. This information might help you to understand what is wrong and to reproduce the issue in your testing environment.
- Sign out after you run the **LoadState** tool. Some settings such as fonts, desktop backgrounds, and screen-saver settings won't take effect until the next time the end user logs on.
- Close all applications before running **ScanState** or **LoadState** tools. If some applications are running during the **ScanState** or **LoadState** process, USMT might not migrate some data. For example, if Microsoft Outlook® is open, USMT might not migrate PST files.

  > **Note**
  >
  > USMT will fail if it can't migrate a file or setting unless you specify the `/c` option. When you specify the `/c` option, USMT ignores errors. However, it logs an error when it encounters a file that is in use that didn't migrate.

User account problems

The following sections describe common user account problems. Expand the section to see recommended solutions.

I'm having problems creating local accounts on the destination computer

Resolution: For more information about creating accounts and migrating local accounts, see Migrate user accounts.

Not all of the user accounts were migrated to the destination computer

Causes/Resolutions There are two possible causes for this problem:

When running the **ScanState** and LoadState tools on Windows 7, Windows 8, or Windows 10, you must run them in Administrator mode from an account with administrative credentials to ensure that all specified users are migrated. To run in Administrator mode:

1. Select **Start** > **All Programs** > **Accessories**.
2. Right-click **Command Prompt**.
3. Select **Run as administrator**.
4. Specify the *LoadState.exe* or *ScanState.exe* command.

If you don't run USMT in Administrator mode, only the user profile that is logged on will be included in the migration.

Any user accounts on the computer that haven't been used won't be migrated. For example, if you add User1 to the computer, but User1 never logs on, then USMT won't migrate the User1 account.

User accounts that I excluded were migrated to the destination computer

Cause: The command that you specified might have had conflicting `ui` and `/ue` options. If a user is specified with the `/ui` option and with either the `/ue` or `/uel` options at the same time, the user will be included in the migration. For example, if you specify `/ui:domain1\* /ue:domain1\user1`, then User1 will be migrated because the `/ui` option takes precedence.

Resolution: For more information about how to use the `/ui` and `/ue` options together, see the examples in the ScanState Syntax article.

I'm using the /uel option, but many accounts are still being included in the migration

Cause: The `/uel` option depends on the last modified date of the users' NTUser.dat file. There are scenarios in which this last modified date might not match the users' last sign-in date.

Resolution: This is a limitation of the `/uel` option. You might need to exclude these users manually with the `/ue` option.

The LoadState tool reports an error as return code 71 and fails to restore a user profile during a migration test

Cause: During a migration test, if you run the **ScanState** tool on your test computer and then delete user profiles in order to test the **LoadState** tool on the same computer, you may have a conflicting key present in the registry. Using the **net use** command to remove a user profile will delete folders and files associated with that profile, but won't remove the registry key.

Resolution: To delete a user profile, use the **User Accounts** item in Control Panel. To correct an incomplete deletion of a user profile:

1. Open the registry editor by typing *regedit.exe* at an elevated command prompt.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`.

   Each user profile is stored in a System Identifier key under `ProfileList`.
3. Delete the key for the user profile you're trying to remove.

Files that weren't encrypted before the migration are now encrypted with the account used to run the LoadState tool

Cause: The **ScanState** tool was run using the `/EFS:copyraw` option to migrate encrypted files and Encrypting File System (EFS) certificates. The encryption attribute was set on a folder that was migrated, but the attribute was removed from file contents of that folder prior to migration.

Resolution: Before using the **ScanState** tool for a migration that includes encrypted files and EFS certificates, you can run the Cipher tool at the command prompt to review and change encryption settings on files and folders. You must remove the encryption attribute from folders that contain unencrypted files or encrypt the contents of all files within an encrypted folder.

To remove encryption from files that have already been migrated incorrectly, you must sign into the computer with the account that you used to run the **LoadState** tool and then remove the encryption from the affected files.

The LoadState tool reports an error as return code 71 and a Windows Error 2202 in the log file

Cause: The computer name was changed during an offline migration of a local user profile.

Resolution: You can use the `/mu` option when you run the **LoadState** tool to specify a new name for the user. For example,

```
cmd

LoadState.exe  /i:MigApp.xml /i:MigDocs.xml \\server\share\migration\mystore
/progress:Progress.log /l:LoadState.log /mu:fareast\user1:farwest\user1
```

Command-line problems

The following sections describe common command-line problems. Expand the section to see recommended solutions.

I received the following error message: "Usage Error: You can't specify a file path with any of the command-line options that exceeds 256 characters."

Cause: You might receive this error message in some cases even if you don't specify a long store or file path, because the path length is calculated based on the absolute path. For example, if you run the `**ScanState**.exe /o store` command from *C:\Program Files\USMT40*, then each character in *C:\Program Files\USMT40* will be added to the length of "store" to get the length of the path.

Resolution: Ensure that the total path length doesn't exceed 256 characters. The total path length includes the store path plus the current directory.

I received the following error message: "USMT was unable to create the log file(s). Ensure that you have write access to the log directory."

Cause: If you're running the **ScanState** or **LoadState** tools from a shared network resource, you'll receive this error message if you don't specify `/l`.

Resolution: To fix this issue in this scenario, specify the `/l:ScanState.log` or `/l:LoadState.log` option.

XML file problems

The following sections describe common XML file problems. Expand the section to see recommended solutions.

I used the `/genconfig` option to create a Config.xml file, but I see only a few applications and components that are in MigApp.xml. Why does Config.xml not contain all of the same applications?

Cause: *Config.xml* will contain only operating system components, applications, and the user document sections that are in both of the .xml files and are installed on the computer when you run the `/genconfig` option. Otherwise, these applications and components won't appear in the *Config.xml* file.

Resolution: Install all of the desired applications on the computer before running the `/genconfig` option. Then run *ScanState.exe* with all of the .xml files. For example, run the following command:

```
cmd

ScanState.exe /genconfig:Config.xml /i:MigDocs.xml /i:MigApp.xml /v:5
/l:ScanState.log
```

I'm having problems with a custom .xml file that I authored, and I can't verify that the syntax is correct

Resolution: You can load the XML schema file *MigXML.xsd* into your XML authoring tool. *MigXML.xsd* is included with USMT. For examples, see the Visual Studio Development Center. Then, load your .xml file in the authoring tool to see if there's a syntax error. For more information about using the XML elements, see USMT XML Reference.

I'm using a MigXML helper function, but the migration isn't working the way I expected it to. How do I troubleshoot this issue?

Cause: Typically, this issue is caused by incorrect syntax used in a helper function. You receive a Success return code, but the files you wanted to migrate didn't get collected or applied, or weren't collected or applied in the way you expected.

Resolution: You should search the **ScanState** or **LoadState** log for either the component name that contains the MigXML helper function, or the MigXML helper function title, so

that you can locate the related warning in the log file.

Migration problems

The following sections describe common migration problems. Expand the section to see recommended solutions.

Files that I specified to exclude are still being migrated

Cause: There might be another rule that is including the files. If there's a more specific rule or a conflicting rule, the files will be included in the migration.

Resolution: For more information, see Conflicts and Precedence and the Diagnostic Log section in Log Files.

I specified rules to move a folder to a specific location on the destination computer, but it hasn't migrated correctly

Cause: There might be an error in the XML syntax.

Resolution: You can use the USMT XML schema (*MigXML.xsd*) to write and validate migration .xml files. Also see the XML examples in the following articles:

Conflicts and precedence

Exclude files and settings

Reroute files and settings

Include files and settings

Custom XML examples

After LoadState completes, the new desktop background doesn't appear on the destination computer

There are three typical causes for this issue.

Cause: Some settings such as fonts, desktop backgrounds, and screen-saver settings aren't applied by **LoadState** until after the destination computer has been restarted.

Resolution: To fix this issue, sign out, and then log back on to see the migrated desktop background.

I included MigApp.xml in the migration, but some PST files aren't migrating

Cause: The *MigApp.xml* file migrates only the PST files that are linked to Outlook profiles.

Resolution: To migrate PST files that aren't linked to Outlook profiles, you must create a separate migration rule to capture these files.

USMT doesn't migrate the Start layout

Description: You're using USMT to migrate profiles from one installation of Windows 10 to another installation of Windows 10 on different hardware. After migration, the user signs in on the new device and doesn't have the Start menu layout they had previously configured.

Cause: A code change in the Start Menu with Windows 10 version 1607 and later is incompatible with this USMT function.

Resolution: The following workaround is available:

1. With the user signed in, back up the Start layout using the following Windows PowerShell command. You can specify a different path if desired:

   ```
   PowerShell
   ```

   ```
   Export-StartLayout -Path "C:\Layout\user1.xml"
   ```

2. Migrate the user's profile with USMT.

3. Before the user signs in on the new device, import the Start layout using the following Windows PowerShell command:

   ```
   PowerShell
   ```

   ```
   Import-StartLayout -LayoutPath "C:\Layout\user1.xml" -MountPath
   %systemdrive%
   ```

This workaround changes the Default user's Start layout. The workaround doesn't scale to a mass migrations or multiuser devices, but it can potentially unblock some scenarios. If other users will sign on to the device, you should delete layoutmodification.xml from the Default user profile. Otherwise, all users who sign on to that device will use the imported Start layout.

Offline migration problems

The following sections describe common offline migration problems. Expand the section to see recommended solutions.

Some of my system settings don't migrate in an offline migration

Cause: Some system settings, such as desktop backgrounds and network printers, aren't supported in an offline migration. For more information, see What does USMT migrate?

Resolution: In an offline migration, these system settings must be restored manually.

The ScanState tool fails with return code 26

Cause: A common cause of return code 26 is that a temp profile is active on the source computer. This profile maps to c:\users\temp. The **ScanState** log shows a **MigStartupOfflineCaught** exception that includes the message **User profile duplicate SID error**.

Resolution: You can reboot the computer to get rid of the temp profile or you can set **MIG_FAIL_ON_PROFILE_ERROR=0** to skip the error and exclude the temp profile.

Include and Exclude rules for migrating user profiles don't work the same offline as they do online

Cause: When offline, the DNS server can't be queried to resolve the user name and SID mapping.

Resolution: Use a Security Identifier (SID) to include a user when running the **ScanState** tool. For example:

```cmd
ScanState.exe /ui:S1-5-21-124525095-708259637-1543119021*
```

The wild card (*) at the end of the SID will migrate the *SID*_Classes key as well.

You can also use patterns for SIDs that identify generic users or groups. For example, you can use the `/ue:*-500` option to exclude the local administrator accounts. For more information about Windows SIDs, see Security identifiers.

My script to wipe the disk fails after running the ScanState tool on a 64-bit system

Cause: The HKLM registry hive isn't unloaded after the **ScanState** tool has finished running.

Resolution: Reboot the computer or unload the registry hive at the command prompt after the **ScanState** tool has finished running. For example, at a command prompt, enter:

```cmd
reg.exe unload hklm\$dest$software
```

Hard-Link Migration Problems

The following sections describe common hard-link migration problems. Expand the section to see recommended solutions.

EFS files aren't restored to the new partition

Cause: EFS files can't be moved to a new partition with a hard link. The `/efs:hardlink` command-line option is only applicable to files migrated on the same partition.

Resolution: Use the `/efs:copyraw` command-line option to copy EFS files during the migration instead of creating hard links, or manually copy the EFS files from the hard-link store.

The ScanState tool can't delete a previous hard-link migration store

Cause: The migration store contains hard links to locked files.

Resolution: Use the UsmtUtils tool to delete the store or change the store name. For example, at a command prompt, enter:

```cmd
UsmtUtils.exe /rd <storedir>
```

You should also reboot the machine.

Related articles

User State Migration Tool (USMT) troubleshooting

Frequently asked questions

Return codes

UsmtUtils syntax

Group Policy troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Group Policy-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Group Policy sub categories

- AppLocker or software restriction policies
- Group Policy management - GPMC or AGPM
- Problems applying Group Policy objects to users or computers

Archived application can't be restored because of app update policies

Article • 12/06/2021 • 2 minutes to read

This article provides a solution to an issue that archived application can't be restored because of app update policies.

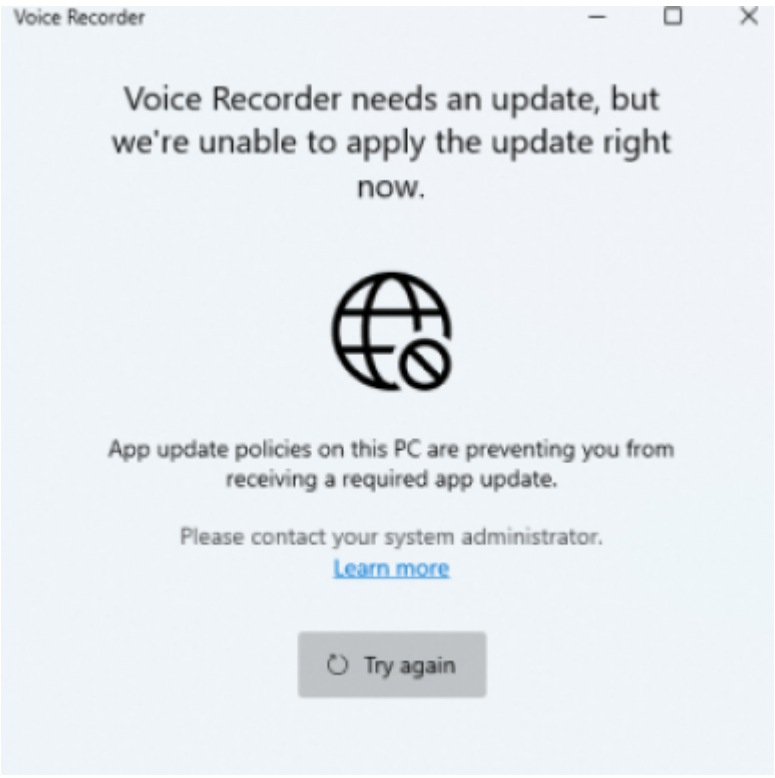
Applies to: Windows 10 - all editions
Original KB number: 4571552

Summary

To reduce disk space usage, Windows automatically archives applications that you don't use frequently. On a new Windows device, some applications are archived out-of-the-box. The first time you start an archived application, the application has to be restored. To do it, it connects to the internet to download and install the full version.

In some environments, Group Policy Objects (GPOs) may block applications from automatically downloading in this manner. When you start such a blocked application, you receive a message that resembles the following.

> Voice Recorder needs an update, but we're unable to apply the update right now.



In these cases, you have to contact your system administrator to obtain an updated version of the application. The information in this article helps you to do this.

More information

The following GPOs prevent archived applications from restoring full versions:

- UpdateServiceUrl
- AllowUpdateService

If either or both of these GPOs are enabled in your environment, your system administrator can use one of the following methods to push the full version of the application to the device:

- If your organization uses Microsoft Store for Business to manage applications, the system administrator can push the application to the business store.
- If your organization uses Microsoft Intune to manage devices, the system administrator can package the application and push the package to managed devices.
- If your organization uses custom Windows images to provision devices, the system administrator can use the DISM App Package tool to add the full resource packages for the application to the image. By using `dism /StubPackageOption:installfull`, the system administrator can make sure that the device is provisioned by using the full version of the application instead of the archived version.

.admx errors when running Local Group Policy Editor (gpedit.msc)

Article • 03/24/2022 • 2 minutes to read

This article provides a workaround for .admx errors when running Local Group Policy Editor (gpedit.msc).

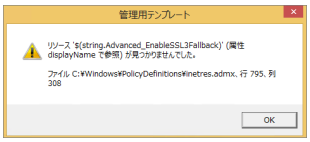
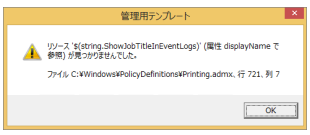
Applies to: Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 3049255

Symptoms

This issue occurs when the following conditions are true:

- You install an additional language pack on a computer.
- You set both the Override for Windows display language and Override for default input method options for the new language under the Advanced settings of the Language in Control Panel.
- You change the system language.

For example, you receive the following error messages when you change to the Japanese language on the computer:

Error files	Text of the errors in Japanese	Screenshot of the errors
InetRes.admx	管理用テンプレート リソース '$(string.Advanced_EnableSSL3Fallback)' (属性 displayName で参照) が見つかりませんでした。ファイル C:\Windows\PolicyDefinitions\inetres.admx、行 795、列 308	
Pinting.admx	管理用テンプレート リソース '$(string.ShowJobTitleInEventLogs)' (属性 displayName で参照) が見つかりませんでした。ファイル C:\Windows\PolicyDefinitions\Printing.admx、行 721、列 7	

Cause

This issue occurs because several system core files have to be updated when they are related to the newly installed language.

Workaround

To work around the issue, reinstall the following update, depending on the error that you receive:

- When you receive the Inetres.admx error, reinstall the update 3021952 that is described in Description of the security update for Internet Explorer: February 10, 2015 (MS15-009).
- When you receive the Printing.admx error, reinstall the update 2934018 that is one of the updates available in Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update: April 2014 (2919355).

> **Note**
>
> - When you install this update (2919355) from Windows Update, updates 2932046, 2937592, 2938439, 2934018, and 2959977 are included in the installation.
> - We recommend that you download and install any needed language pack before you install updates.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the "Applies to" section.

Can't disable Microsoft Store in Windows 10 Pro through Group Policy

Article • 09/23/2021 • 2 minutes to read

This article describes an issue that prevents you from using Group Policy to disable the Windows Store app on a computer that's running Windows 10 Pro.

Applies to: Windows 10, version 1903, Windows 10, version 1809
Original KB number: 3135657

Symptoms

On a computer that's running Windows 10 Pro, you upgrade to Windows 10, version 1511, Windows 10, version 1809 or Windows 10, version 1903. After the upgrade, you notice that the following Group Policy settings to disable Microsoft Store are not applied, and you cannot disable Microsoft Store:

- **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Store** > **Turn off the Store application**
- **User Configuration** > **Administrative Templates** > **Windows Components** > **Store** > **Turn off the Store**

Cause

This behavior is by design. In Windows 10, version 1511, Windows 10, version 1809, and Windows 10, version 1903, these policies are applicable to users of the Enterprise and Education editions only.

How to create and manage the Central Store for Group Policy Administrative Templates in Windows

Article • 10/21/2022 • 6 minutes to read

This article describes how to use the new .admx and .adml files to create and administer registry-based policy settings in Windows. This article also explains how the Central Store is used to store and to replicate Windows-based policy files in a domain environment.

Applies to: Windows 11, Windows 10 - all editions, Windows Server 2019, Windows Server 2012 R2, Windows 7 Service Pack 1
Original KB number: 3087759

Links to download the Administrative Templates files based on the operating system version

- Administrative Templates (.admx) for Windows 11 2022 Update (22H2)
- Administrative Templates (.admx) for Windows 11 October 2021 Update (21H2)
- Administrative Templates (.admx) for Windows 10 November 2021 Update (21H2) - v2.0
- Administrative Templates (.admx) for Windows 10 November 2021 Update (21H2)
- Administrative Templates (.admx) for Windows 10 May 2021 Update (21H1)
- Administrative Templates (.admx) for Windows 10 October 2020 Update (20H2) - v2.0
- Administrative Templates (.admx) for Windows 10 May 2020 Update (2004)
- Administrative Templates (.admx) for Windows 10 November 2019 Update (1909)
- Administrative Templates (.admx) for Windows 10 May 2019 Update (1903)
- Administrative Templates (.admx) for Windows 10 October 2018 Update (1809)
- Administrative Templates (.admx) for Windows 10, version 1803 (April 2018 Update)
- Administrative Templates (.admx) for Windows 10, version 1709 (Fall Creators Update)

- Administrative Templates (.admx) for Windows 10, version 1703 (Creators Update)
- Administrative Templates (.admx) for Windows 10, version 1607 and Windows Server 2016
- Administrative Templates (.admx) for Windows 10 and Windows 10, version 1511
- Administrative Templates (.admx) for Windows 8.1 Update and Windows Server 2012 R2 Update
- Administrative Templates (.admx) for Windows 8.1 and Windows Server 2012 R2

To view ADMX spreadsheets of the new settings that are available in later operating system versions, see Group Policy Settings Reference Spreadsheet for Windows 10 November 2021 Update (21H2).

Overview

Administrative Templates files are divided into .admx files and language-specific .adml files for use by Group Policy administrators. The changes that are implemented in these files let administrators configure the same set of policies by using two languages. Administrators can configure policies by using the language-specific .adml files and the language-neutral .admx files.

Administrative Templates file storage

Windows uses a Central Store to store Administrative Templates files. The ADM folder is not created in a Group Policy Object (GPO) as it is done in earlier versions of Windows. Therefore, Windows domain controllers do not store or replicate redundant copies of .adm files.

The Central Store

To take advantage of the benefits of .admx files, you must create a Central Store in the sysvol folder on a Windows domain controller. The Central Store is a file location that is checked by the Group Policy tools by default. The Group Policy tools use all .admx files that are in the Central Store. The files that are in the Central Store are replicated to all domain controllers in the domain.

We suggest keeping a repository of any ADMX/L files that you have for applications that you may want to use. For example, operating system extensions like Microsoft Desktop optimization Pack (MDOP), Microsoft Office, and also third-party applications that offer Group Policy support.

To create a Central Store for .admx and .adml files, create a new folder named PolicyDefinitions in the following location (for example) on the domain controller:

`\\contoso.com\SYSVOL\contoso.com\policies\PolicyDefinitions`

When you already have such a folder that has a previously built Central Store, use a new folder describing the current version such as:

`\\contoso.com\SYSVOL\contoso.com\policies\PolicyDefinitions-1803`

Copy all files from the PolicyDefinitions folder on a source computer to the new PolicyDefinitions folder on the domain controller. The source location can be either of the following ones:

- The `C:\Windows\PolicyDefinitions` folder on a Windows 8.1-based or Windows 10-based client computer
- The `C:\Program Files (x86)\Microsoft Group Policy\<version-specific>\PolicyDefinitions` folder, if you have downloaded any of the Administrative Templates separately from the links above.

The PolicyDefinitions folder on the Windows domain controller stores all .admx files and .adml files for all languages that are enabled on the client computer.

The .adml files are stored in a language-specific folder. For example, English (United States).adml files are stored in a folder that is named *en-US*. Korean .adml files are stored in a folder that is named *ko_KR*, and so on.

If .adml files for additional languages are required, you must copy the folder that contains the .adml files for that language to the Central Store. When you have copied all .admx and .adml files, the PolicyDefinitions folder on the domain controller should contain the .admx files and one or more folders that contain language-specific .adml files.

> ⓘ **Note**
>
> When you copy the .admx and .adml files from a Windows 8.1-based or Windows 10-based computer, verify that the most recent updates to these files are installed. Also, make sure that the most recent Administrative Templates files are replicated. This advice also applies to service packs, as applicable.

When the operating system collection is completed, merge any OS extension or application ADMX/ADML files into the new PolicyDefinitions folder.

When this is finished, rename the current PolicyDefinitions folder to reflect that it's the previous version, such as PolicyDefinitions-1709. Then, rename the new folder (such as PolicyDefinitions-1803) to the production name.

We suggest this approach as you can revert to the old folder in case you experience a severe problem with the new set of files. When you don't experience any problems with the new set of files, you can move the older PolicyDefinitions folder to an archive location outside sysvol folder.

Group Policy administration

Windows 8.1 and Windows 10 do not include Administrative Templates that have an .adm extension. We recommend that you use computers that are running Windows 8.1 or later versions of Windows to perform Group Policy administration.

Updating the Administrative Templates files

In Group Policy for Windows Vista and later version of Windows, if you change Administrative Templates policy settings on local computers, sysvol folder isn't automatically updated to include the new .admx or .adml files. This behavior is implemented to reduce network load and disk storage requirements, and to prevent conflicts between .admx and .adml files when changes are made to Administrative Templates policy settings across different locations.

To ensure that any local updates are reflected in sysvol folder, you must manually copy the updated .admx or .adml files from the PolicyDefinitions file on the local computer to the Sysvol\PolicyDefinitions folder on the appropriate domain controller.

The following update enables you to configure the Local Group Policy editor to use Local .admx files instead of the Central Store:

An update is available to enable the use of Local ADMX files for Group Policy Editor.

You can also use this setting to:

- Test a newly built folder as `C:\Windows\PolicyDefinitions` on an Administrative Workstation against your Domain Policies, before you copy it to the Central Store on sysvol folder.
- Use older PolicyDefinitions folder to edit policy settings that don't have an ADMX file in the latest build of your Central Store. One common example would be policies that have settings for older versions of Microsoft Office that are still in the Group Policies. Microsoft Office has a separate set of ADMX/L files for each release.

Known Issues

- Issue 1

  After you copy the Windows 10 .admx templates to the sysvol folder Central Store and overwrite all existing .admx and .adml files, select the **Policies** node under **Computer Configuration** or **User Configuration**. In this situation, you may receive the following error message:

  > Namespace 'Microsoft.Policies.Sensors.WindowsLocationProvider' is already defined as the target namespace for another file in the store.
  > File
  > \\<forest.root>\SysVol<forest.root>\Policies\PolicyDefinitions\Microsoft-Windows-Geolocation-WLPAdm.admx, line 5, column 110

  > **Note**
  >
  > In the path in this message, **<forest.root>** represents the domain name.

  To resolve this problem, see "'Microsoft.Policies.Sensors.WindowsLocationProvider' is already defined" error when you edit a policy in Windows.

- Issue 2

  Updated ADMX/L files for Windows 10 version 1803 contain only SearchOCR.ADML. It is not compatible with an older release of SearchOCR.ADMX that you still have in the Central Store. For more information about the problem, see "Resource '$(string ID=Win7Only)' referenced in attribute displayName could not be found" error when you open gpedit.msc in Windows.

  Both issues can be avoided by building a pristine PolicyDefinitions folder from a base OS release folder as described above.

Logon scripts don't run for five minutes after a user logs on to a Windows 8.1-based computer

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where logon scripts don't run for five minutes after a user logs on to a Windows 8.1-based computer.

Applies to: Windows 10 - all editions
Original KB number: 2895815

Symptoms

After a user logs on to a Windows 8.1-based computer, the logon scripts do not run for five minutes. This behavior causes the following symptoms to occur:

- Operations that are performed by the logon scripts may not be visible on Windows 8.1-based computers until five minutes after the user logs on.
- Resources that are made available by the logon scripts may not be available to users on Windows 8.1-based computers until about five minutes after users log on.

Cause

This behavior occurs because Windows 8.1 includes a new Group Policy setting, **Configure Logon Script Delay**, that controls the behavior of logon scripts. This script is stored in the following location:

Computer Configuration\Administrative Templates\System\Group Policy

The default value setting for the **Configure Logon Script Delay** policy is **Not Configured**. However, the default behavior of a Group Policy client is to wait five minutes before it runs logon scripts.

The goal of the five-minute delay is to speed up the loading of the user's desktop on Windows 8.1-based computers.

Resolution

If you want the logon scripts to run at user logon without any delay, you should configure the **Configure Logon Script Delay** setting to **Disabled** in the Computer Configuration\Administrative Templates\System\Group Policy location.

If you want to change the time that the Group Policy client waits until it runs the logon scripts, you should configure the **Configure Logon Script Delay** setting to **Enabled** in the Computer Configuration\Administrative Templates\System\Group Policy location. Then, in the options section, set **minute** to the desired value. The maximum value that you can enter is 1,000 minutes.

After you set the policy to **Enabled** and set the time in minutes, the Group Policy client waits for the specified time before it runs logon scripts at user logon. If you enter the time in minutes as zero (0), the setting is disabled, and the Group Policy client runs the logon scripts at user logon without any delay.

Use the Settings app Group Policy in Windows 10

Article • 12/06/2021 • 2 minutes to read

Applies to: Windows 10 - all editions
Original KB number: 4019502

Overview

Windows 10, version 1703, and later versions introduce Group Policies to manage access to the Settings app pages. It enables IT Administrators to hide pages from users that they don't want them to access while still enabling access to pages that they want or need users to access. Before Windows 10, version 1703, Administrators could only fully lock down the Settings app or enable full access.

Settings app

Each Settings app page has a URI that can be used to identify the page programmatically. It's how the Settings app Group Policy knows which page to enable or block access to. An administrator will use the URI of the page to tell the Group Policy what page or pages they want to control. For a full list of ms-settings URIs, see MS-Settings URI Scheme Reference.

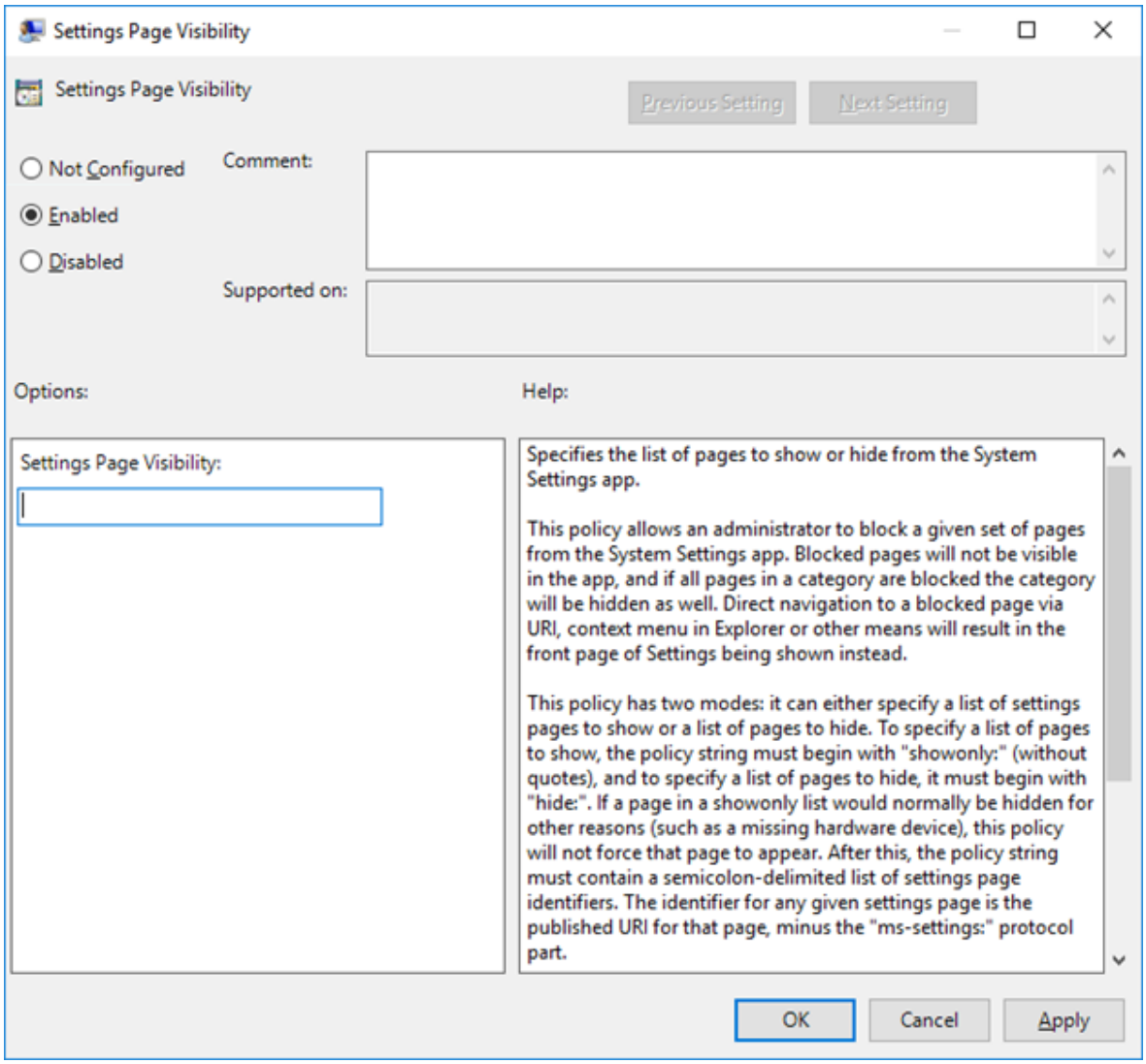
Settings app Group Policy

The Settings app Group Policy has two modes. An administrator can either specify a list of Settings app pages to show or a list of Settings app pages to hide. You do so by enabling the Group Policy, and specifying a multi-string value that begins either with **ShowOnly:** or **Hide:** followed by a semicolon-delimited list of the Settings app pages.

Use Setting app Group Policy

1. Open the Local Group Policy Editor and then go to **Computer Configuration** > **Administrative Templates** > **Control Panel**.

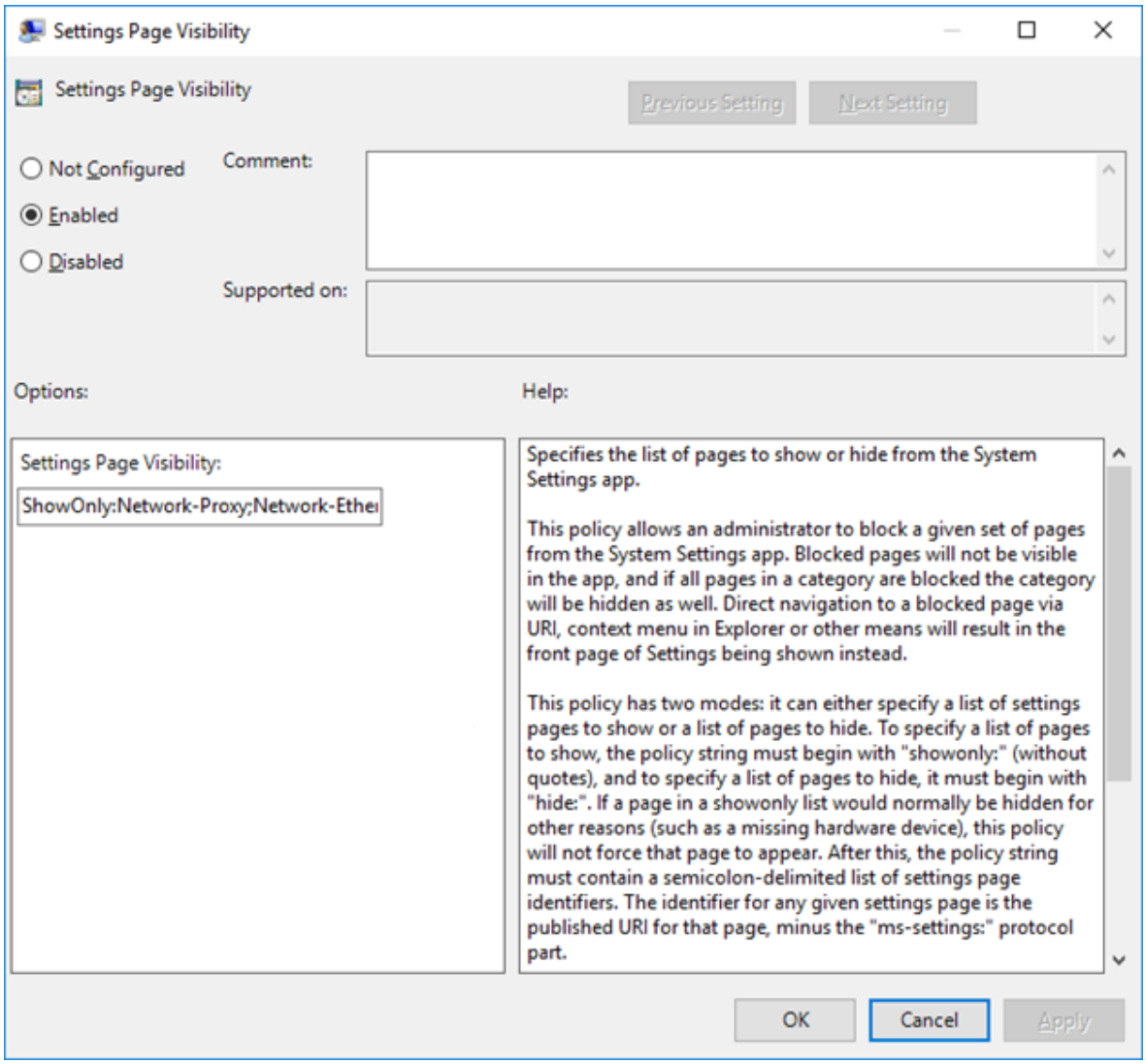
2. Double-click the **Settings Page Visibility** policy and then select **Enabled**.



3. Depending on your need, specify either a **ShowOnly:** or **Hide:** string.

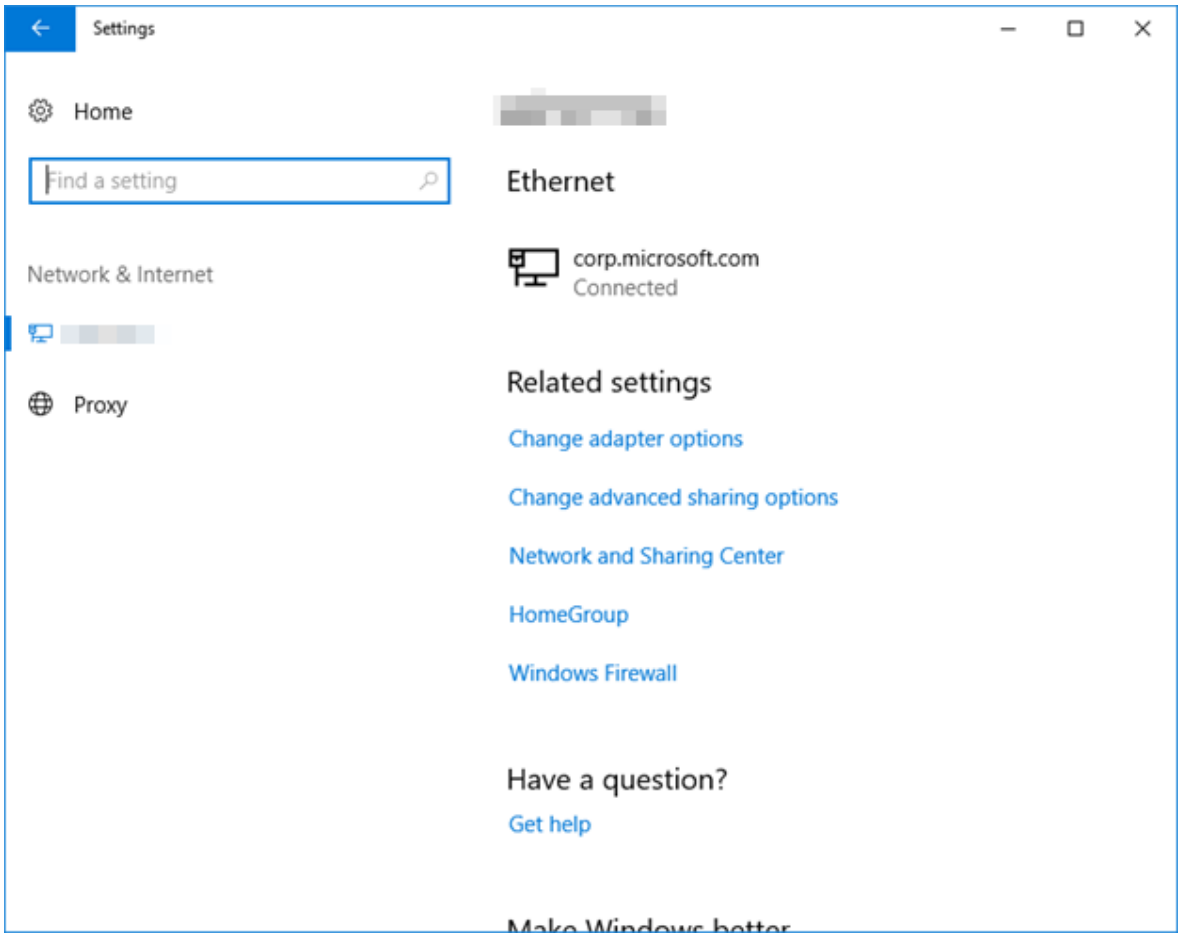
   If you want to show only Proxy and Ethernet, the string would be as follows:

   `ShowOnly:Network-Proxy;Network-Ethernet`



If you want to hide Proxy and Ethernet, but enable access to everything else, the string would be as follows:

```
Hide:Network-Proxy;Network-Ethernet
```



Determine the URI of a Settings app page

To determine the URI of a Settings app page, look up the URI on the ms-settings: URI scheme reference page.

For example, if you must control access to the Mobile hotspot settings, locate the Mobile hotspot entry on the webpage. The URI is `ms-settings:network-mobilehotspot`. Remove the **ms-settings:** part of the string. To restrict access to the Mobile hotspot settings page only, set your string as `Hide:network-mobilehotspot`.

If you must restrict more than one page, you must use a semicolon between each URI. For example, to restrict access to Mobile hotspot and Proxy, you would specify the following string:
`Hide:network-mobilehotspot;network-proxy`

Using Group Policy Objects to hide specified drives

Article • 09/23/2021 • 4 minutes to read

This article provides some information about using Group Policy Objects to hide specified drives.

Applies to: Windows 10 - all editions
Original KB number: 231289

Summary

With Group Policy Objects in Windows, there is a "Hide these specified drives in My Computer" option that lets you hide specific drives. However, it may be necessary to hide only certain drive, but retain access to others.

There are seven default options for restricting access to drives. You can add other restrictions by modifying the System.adm file for the default domain policy or any custom Group Policy Object (GPO). The seven default selections are:

- Restrict A, B, C and D drives only
- Restrict A, B and C drives only
- Restrict A and B drives only
- Restrict all drives
- Restrict C drive only
- Restrict D drive only
- Do not restrict drives

Microsoft does not recommend to change the System.adm file, but instead to create a new .adm file and import this .adm into the GPO. The reason is that if you apply changes to the system.adm file, these changes might get overwritten if Microsoft releases a new version of the system.adm file in a Service Pack.

More Information

The default location of the System.adm file for a default domain policy is:

%SystemRoot%\Sysvol\Sysvol\<YourDomainName>\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Adm\System.adm

The contents of these folders are replicated throughout a domain by the File Replication service (FRS).

> ⓘ **Note**
>
> The Adm folder and its contents are not populated until the default domain policy is loaded for the first time.

To make changes to this policy for one of the seven default values:

1. Start the Microsoft Management Console. On the Console menu, click **Add/Remove Snap-in**.
2. Add the Group Policy snap-in for the default domain policy. To do this, click **Browse** when you are prompted to select a Group Policy Object (GPO). The default GPO is Local Computer. You can also add GPOs for other domain partitions (specifically, Organizational Units).
3. Open the following sections: **User Configuration**, **Administrative Templates**, **Windows Components**, and **Windows Explorer**.
4. Click **Hide these specified drives in My Computer**.
5. Click to select the **Hide these specified drives in My Computer** check box.
6. Click the appropriate option in the drop-down box.

These settings remove the icons representing the selected hard disks from My Computer, Windows Explorer, and My Network Places. Also, these drives do not appear in the Open dialog box of any programs.

This policy is designed to protect certain drives, including the floppy disk drive, from misuse. It can also be used to direct users to save their work to certain drives.

To use this policy, select a drive or combination of drives in the drop-down box. To display all drives (hide none), disable this policy or click the **Do not restrict drives** option.

This policy does not prevent users from using other programs to gain access to local and network drives or prevent them from viewing and changing drive characteristics by using the Disk Management snap-in.

The default values are not the only values that you can use. By editing the System.adm file, you can add your own custom values. This is the portion of the System.adm to be modified:

```
Output
```

```
POLICY !!NoDrives
     EXPLAIN !!NoDrives_Help
        PART !!NoDrivesDropdown DROPDOWNLIST NOSORT REQUIRED
           VALUENAME "NoDrives"
            ITEMLIST
                  NAME !!ABOnly VALUE NUMERIC 3
                  NAME !!COnly VALUE NUMERIC 4
                  NAME !!DOnly VALUE NUMERIC 8
                  NAME !!ABConly VALUE NUMERIC 7
                  NAME !!ABCDOnly VALUE NUMERIC 15
                  NAME !!ALLDrives VALUE NUMERIC 67108863
                  ;low 26 bits on (1 bit per drive)
                  NAME !!RestNoDrives VALUE NUMERIC 0 (Default)
            END ITEMLIST
        END PART
      END POLICY

[strings]
ABCDOnly="Restrict A, B, C and D drives only"
ABConly="Restrict A, B and C drives only"
ABOnly="Restrict A and B drives only"
ALLDrives="Restrict all drives"
COnly="Restrict C drive only"
DOnly="Restrict D drive only"
RestNoDrives="Do not restrict drives"
```

The [strings] section represents substitutions of the actual values in the drop-down box.

This policy displays only specified drives on the client computer. The registry key that this policy affects uses a decimal number that corresponds to a 26-bit binary string, with each bit representing a drive letter:

11111111111111111111111111 ZYXWVUTSRQPONMLKJIHGFEDCBA

This configuration corresponds to 67108863 in decimal and hides all drives. If you want to hide drive C, make the third-lowest bit a 1, and then convert the binary string to decimal.

It is not necessary to create an option to show all drives, because clearing the check box deletes the "NoDrives" entry entirely, and all drives are automatically shown.

If you want to configure this policy to show a different combination of drives, create the appropriate binary string, convert to decimal, and add a new entry to the ITEMLIST section with a corresponding [strings] entry. For example, to hide drives L, M, N, and O, create the following string

00000000000111100000000000 ZYXWVUTSRQPONMLKJIHGFEDCBA

and convert to decimal. This binary string converts to 30720 in decimal. Add this line to the [strings] section in the System.adm file:

LMNO_Only="Restrict L, M, N and O drives only"

Add this entry in the ITEMLIST section above and save the System.adm file.

NAME !!LMNO_Only VALUE NUMERIC 30720

This creates an eighth entry in the drop-down box to hide drives L, M, N, and O only. Use this method to include more values in the drop-down box. The modified section of the System.adm file appears as follows:

Output

```
POLICY !!NoDrives
     EXPLAIN !!NoDrives_Help
        PART !!NoDrivesDropdown DROPDOWNLIST NOSORT REQUIRED
           VALUENAME "NoDrives"
            ITEMLIST
                  NAME !!ABOnly VALUE NUMERIC 3
                  NAME !!COnly VALUE NUMERIC 4
                  NAME !!DOnly VALUE NUMERIC 8
                  NAME !!ABConly VALUE NUMERIC 7
                  NAME !!ABCDOnly VALUE NUMERIC 15
                  NAME !!ALLDrives VALUE NUMERIC 67108863
                  ;low 26 bits on (1 bit per drive)
                  NAME !!RestNoDrives VALUE NUMERIC 0 (Default)
                              NAME !!LMNO_Only VALUE NUMERIC 30720
            END ITEMLIST
       END PART
     END POLICY

[strings]
ABCDOnly="Restrict A, B, C and D drives only"
ABConly="Restrict A, B and C drives only"
ABOnly="Restrict A and B drives only"
ALLDrives="Restrict all drives"
COnly="Restrict C drive only"
DOnly="Restrict D drive only"
RestNoDrives="Do not restrict drives"
LMNO_Only="Restrict L, M, N and O drives only"
```

This [strings] section represents substitutions of the actual values in the drop-down box.

Error when you open gpedit.msc: Resource $(string id="Win7Only)' referenced in attribute displayName could not be found

Article • 11/26/2021 • 2 minutes to read

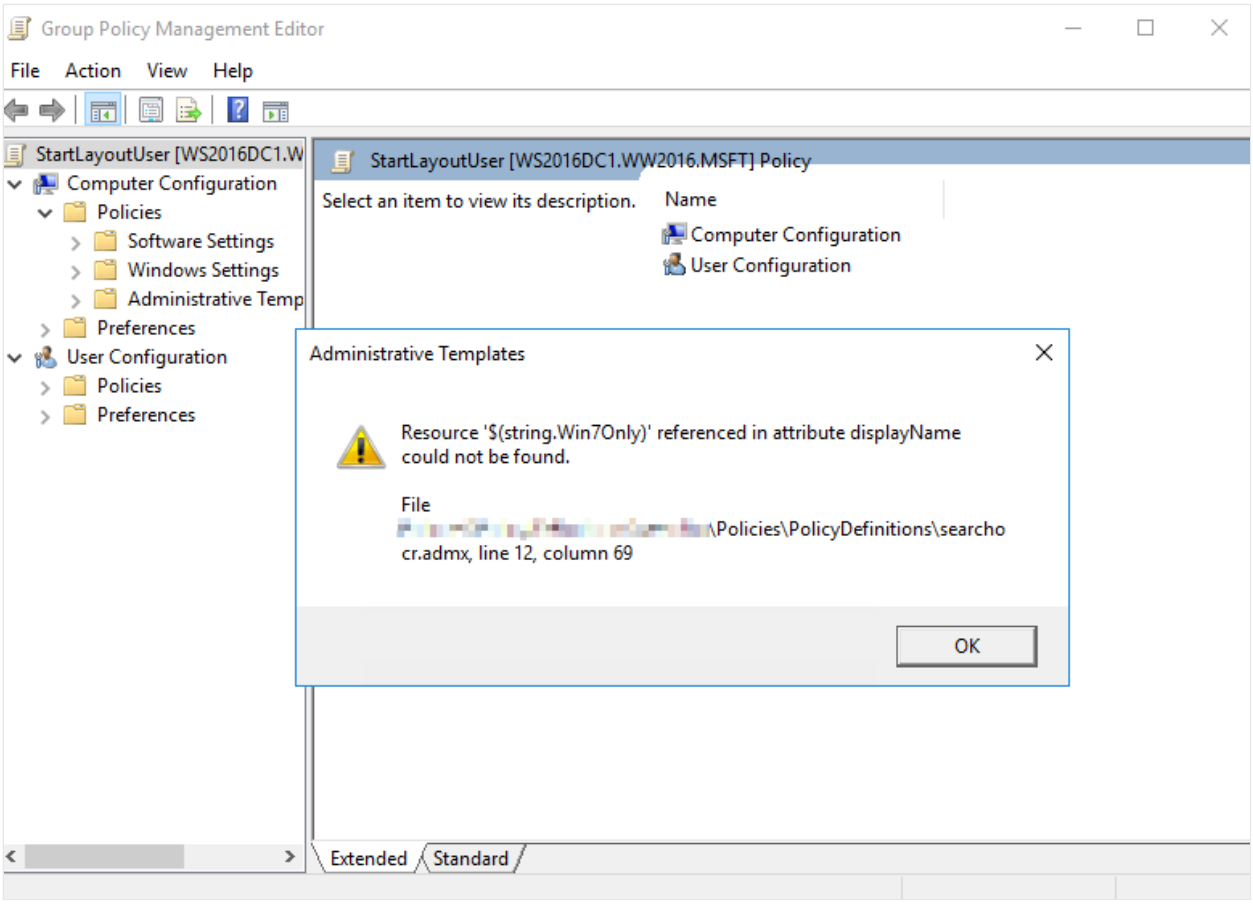
This article provides help to solve an issue where you receive an error (Resource $(string id="Win7Only)' referenced in attribute displayName could not be found) when you open gpedit.msc.

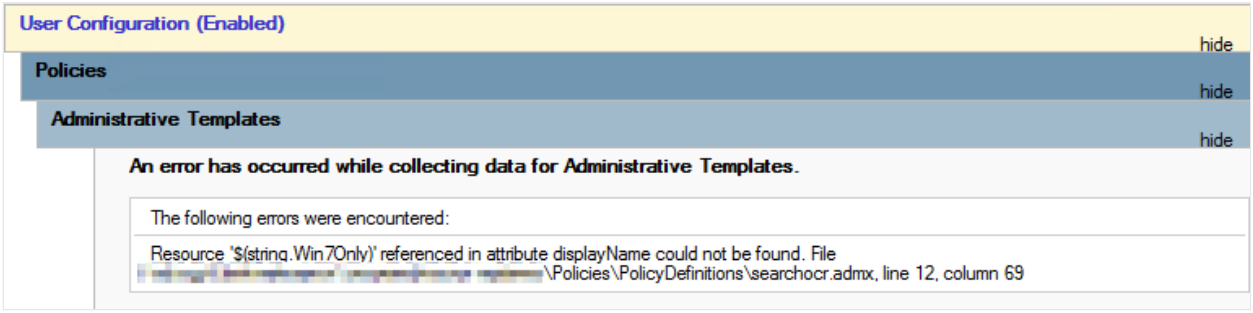
Applies to: Windows 10, version 1803
Original KB number: 4292332

Symptom

Assume that you update the ADML and ADMX file to the Windows 10, version 1803 version. When you open gpedit.msc, you receive the following error:

> Resource $(string id="Win7Only)' referenced in attribute displayName could not be found





Cause

This is a known issue. There are text updates in the Windows 10, version 1803 version of SearchOCR.ADML. However, when the changes were made, this line was cut-out of the new ADML:

```
\<string id="Win7Only">Microsoft Windows 7 or later\</string>
```

Resolution

To fix this issue, download the updated ADMX package by using the following link. Then, use the updated SearchOCR.ADMX and SearchOCR.ADML files from it.

Administrative Templates (.admx) for Windows 10 April 2018 Update (1803)

Workarounds

To work around this issue, follow these steps:

1. Add the missing String to the 1803 version of SearchOCR.adml.
2. Copy the old Windows 10, version 1511 version of SearchOCR.admx to the system. This file was not updated after Windows 10, version 1511 until the Windows 10, version 1803 release.

To update SearchOCR.adml, follow these steps:

> ⓘ **Note**
>
> This is for the United States English version. Other languages will have similar instructions.

1. Locate the file in the `\path\PolicyDefinitions\en-US` folder.
2. Make a backup copy of SearchOCR.adml in case that you make a mistake when editing the file.
3. Open the file in a text editor. (If you use notepad.exe, turn on the **Status** Bar on the **View** menu.)
4. Locate line 26.
5. Add a blank line. Line 26 should now be blank.
6. On the blank line 26 paste this text:

   ```
   \<string id="Win7Only">Microsoft Windows 7 or later\</string>
   ```

7. Save the file.

Windows 7 Clients intermittently fail to apply group policy at startup

Article • 09/23/2021 • 3 minutes to read

This article provides a solution to an issue where Windows 7 Clients intermittently fail to apply group policy at startup.

Applies to: Windows 7 Service Pack 1
Original KB number: 2421599

Symptoms

Windows 7 clients intermittently fail group policy processing at startup or reboot. The following events are logged in the System event log:

> Error 9/9/2010 2:43:29 PM NETLOGON 5719 Error 9/9/2010 2:43:31 PM GroupPolicy 1055

Cause

The behavior is caused by a race condition between network initialization, locating a Domain Controller and processing Group Policy. If the network isn't available, a Domain Controller won't be located, and Group Policy processing will fail. Once the operating system has loaded and a network link is negotiated and established, background refresh of Group Policy will succeed.

The following sequence of events reflects the condition:

> Information <DateTime> EventLog 6006 indicates system shutdown
> Information <DateTime> e1kexpress 33 indicates that your network connection link has been established with <speed/duplex>
> Information <DateTime> EventLog 6005 indicates event log service has started
> Information <DateTime> Dhcp-Client 50036 indicates dhcp client service has started
> Error <DateTime> NETLOGON 5719 indicates netlogon unable to reach any of the domain controllers
> Error <DateTime> GroupPolicy 1055 indicates group policy processing failed
> Information <DateTime> GroupPolicy 1503 indicates group policy processing succeeded

It can be confirmed via the `netlogon` logs as well:

> <DateTime> [SESSION] \Device\NetBT_Tcpip_{53267BA1-EB8C-4348-BD81-41C3FF162EE9}: Transport Added (<IP Address>) <DateTime> [SESSION] Winsock Addrs: <IP Address> (1) Address changed. <DateTime> [CRITICAL] NetpDcGetDcNext: _ldap._tcp.dc._msdcs.contoso.com.: Cannot Query DNS. 1460 0x5b4 <DateTime> [CRITICAL] NetpDcGetNameIp: `contoso.com`.: No data returned from DnsQuery. <DateTime> [CRITICAL] DBG: NlDiscoverDc: Cannot find DC. <DateTime> [CRITICAL] DBG: NlSessionSetup: Session setup: cannot pick trusted DC <DateTime> [SESSION] DBG: NlSetStatusClientSession: Set connection status to c000005e <DateTime> [SESSION] DBG: NlSessionSetup: Session setup Failed

Resolution

To work around the issue, you can set a registry value to delay the application of Group Policy:

1. Open Registry Editor.
2. Expand the following subkey: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`
3. Right-click `Winlogon`, point to **New**, and then select **DWORD Value**.
4. To name the new entry, type `GpNetworkStartTimeoutPolicyValue`, and then press ENTER.
5. Right-click `GpNetworkStartTimeoutPolicyValue`, and then select **Modify**.
6. Under **Base**, select **Decimal**.
7. In the Value data box, type **60**, and then select **OK**.
8. Quit Registry Editor, and then restart the computer.
9. If the Group Policy startup script doesn't run, increase the value of the `GpNetworkStartTimeoutPolicyValue` registry entry.

More information

The value specified should be sufficiently long enough to ensure that the connection is made. During the timeout period, Windows will check the connection status every two seconds and will continue with system startup as soon as the connection is confirmed.

Therefore, erring on the high side is recommended. If the system is legitimately disconnected (for example, disconnected network cable, off-line server, and so on), Windows will stall for the entire timeout period.

It can also be defined via a Group Policy:

Policy Location: Computer Configuration > Policies > Admin Templates > System > Group Policy Setting Name: Startup policy processing wait time Registry Key: `HKLM\Software\Policies\Microsoft\Windows\System!GpNetworkStartTimeoutPolicyValue`

If you define the Group policy setting, it would override the manual setting. When manual and Group Policy setting aren't defined, the value is picked from the following registry location:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\History`

Since there's no time-out period defined, the system uses its own algorithm to calculate and arrive at an Average time-out period. This value is stored in the above registry location. It could vary system to system, and depends on various factors, such as previous login attempts.

> ⓘ **Note**
>
> The Group Policy description for "Startup Policy processing wait time" is not verbose and doesn't cover all scenarios. Just because we don't have the policy configured currently doesn't mean that we are going to use a default time-out value of 30 seconds.

Disable screen saver passwords by using policies

Article • 09/23/2021 • 2 minutes to read

This article describes how to make screen saver password locks unavailable on systems in a site, domain, or organizational unit, by using the policies available.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 272304

Disable screen saver passwords

To make screen saver password locks unavailable, follow these steps:

1. Click Start, and then click **Run**.
2. Type *mmc*, and then click **OK** to start the Microsoft Management Console (MMC).
3. On the Console menu, click **Add/Remove Snap-ins**, and then click **Add**.
4. Click **Group Policy**, and then click **Add**.

   The **Select Group Policy Object** dialog box appears. If you want to apply this policy only to your computer, make sure that your local computer is listed in the Group Policy object, and then click **Finish**.

   Alternatively, if this will be an Active Directory policy, click **Browse**, select the site, domain, or organizational unit to which you want this policy to apply, and then click **Finish**.
5. Click **Close**.
6. Expand **User Configuration**, and then expand **Administrative Templates**.
7. Expand **Control Panel**, and then click **Display**.
8. In the right pane, double-click **Password protect the screen saver**.
9. Select Disable on the **Policy** tab. This prevents users from setting passwords on screen savers for this computer or domain.
10. Click the **Explain** tab for information about how to use this policy.
11. Click **Apply**.

12. Click **OK**, and then close the MMC.

Group membership changes don't update over some VPN connections

Article • 11/04/2021 • 13 minutes to read

This article describes a situation in which VPN users might experience resource access or configuration problems after their group membership changes.

Applies to: Windows 10, all SACs

Symptoms

In response to the Covid-19 pandemic, an increasing number of users now work, learn, and socialize from home. They connect to the workplace by using VPN connections. These VPN users report that when they are added to or removed from security groups, the changes might not take effect as expected. They report symptoms such as the following:

- Changes to network resource access don't take effect.
- Group Policy Objects (GPOs) that target specific security groups don't apply correctly.
- Folder Redirection policy isn't applied correctly.
- Applocker rules that target specific security groups don't work.
- Logon scripts that create mapped drives, including user home folder or GPP drive maps, don't work.
- The `whoami /groups` command (run at a command prompt) reports an out-of-date list of group memberships for the user's local security context.
- The `gpresult /r` command (run at a command prompt) reports an out-of-date list of group memberships.

If the user locks and then unlocks Windows while the client remains connected to the VPN, some of these symptoms resolve themselves. For example, some resource access changes take effect. Subsequently, if the user signs out of Windows and then signs back in (closing all sessions that use network resources), more of the symptoms resolve. However, logon scripts might not function correctly, and the `gpresult /r` command might still not reflect group membership changes. The user cannot work around the problem by using the `runas` command to start a new Windows session on the client. This command just uses the same credential information to start the new session.

The scope of this article includes environments that have implemented Authentication Mechanism Assurance (AMA) in the domain, and in which users have to authenticate by

using a Smart Card to access network resources. For more information, see Description of AMA usage in interactive logon scenarios in Windows.

Cause

In an office environment, it's common for a user to sign out of Windows at the end of the workday. When the user signs in the next day, the client is already connected to the network and has direct access to a domain controller. Under these conditions, changes to group membership take effect quickly. The user has the correct access levels the next day (the next time the user signs in). Similarly, changes to Group Policy appear to take effect within a day or two (after the user signs in one or two times, depending on the policies that are scheduled to apply).

In a home environment, the user might disconnect from the VPN at the end of the workday and lock Windows. They might not sign out. When the user unlocks Windows (or signs in) the next morning, the client doesn't connect to the VPN (and doesn't have access to a domain controller) until after the user has unlocked Windows or signed in. The client signs the user in to Windows by using cached credentials instead of by contacting the domain controller for fresh credentials. Windows builds a security context for the user that is based on the cached information. Windows also applies Group Policy asynchronously, based on the local Group Policy cache. This usage of cached information can cause the following behavior:

- The user may have access to resources they shouldn't have, and may not have access to resources that they should have.
- Group Policy settings may not be applied as expected, or the Group Policy settings may be out-of-date.

This behavior occurs because Windows uses cached information to improve performance when users sign in. Windows also uses cached information to sign in users on domain-joined clients that are not connected to the network. Unexpected consequences occur if the client exclusively uses a VPN to connect to the network, and the client cannot establish the VPN connection until after the user signs in.

> **Important**
>
> This behavior is relevant only in the interactive logon scenario. Access to network resources works as expected because the network logon does not use cached information. Instead, the group information comes from a domain controller query.

Effects on the user security context and access control

If the client cannot connect to a domain controller when the user signs in, Windows bases the user security context on cached information. After Windows creates the user security context, it does not update the context until the next time that the user signs in.

For example, suppose that a user is assigned to a group in Active Directory while the user is offline. The user signs in to Windows, and then connects to the VPN. If the user opens a Command Prompt window and then runs the `whoami /groups` command, the list of groups doesn't include the new group. The user locks and then unlocks the desktop while still connected to the VPN. The `whoami /groups` command still produces the same result. Finally, the user signs out of Windows. After the user signs in again, the `whoami /groups` command produces the correct result.

The effect of the cached information on the user's access to resources depends on the following factors:

- **Whether the resources are on the client or on the network**
  Resources on the network require an additional authentication step (a network logon instead of an interactive logon). This step means that the group information that the resource uses to determine access always comes from a domain controller, not the client cache.
- **Whether the resources use Kerberos tickets or other technologies (such as NTLM access tokens) to authenticate and authorize users**
  - For details about how cached information affects user access to NTLM-secured resources, see Resources that rely on NTLM authentication.
  - For details about how cached information affects user access to Kerberos-secured resources, see Resources that rely on Kerberos tickets.
- **Whether the user is resuming an existing resource session or starting a new resource session**
- **Whether the user locks and unlocks the client while connected to the VPN**
  If the user locks the client while connected to the VPN and then unlocks it, the client updates its cache of user groups. However, this change does not affect the existing user security context or any sessions that were running when the user locked the client.
- **Whether the user signs out of the client while connected to the VPN, and then signs in again**
  The effects of signing out and then signing in differ depending on whether the user has locked and unlocked the client first while connected to the VPN. Locking the client and then unlocking it updates the cache of user information that the client uses at the next sign-in.

Resources that rely on NTLM authentication

This category of resources includes the following:

- The user session on the client
- Any resource sessions on the client that rely on NTLM authentication
- Any resource sessions on the network that rely on NTLM authentication

> **Important**
>
> When the user accesses a resource on the network that requires NTLM authentication, the client presents cached credentials from the user security context. However, the resource server queries the domain controller for the most recent user information.

These resource sessions, including the user session on the client, do not expire. They continue to run until the user ends the session, such as when the user signs out of Windows. Locking and then unlocking the client does not end the existing sessions.

Resources that rely on Kerberos tickets

When the user connects to the VPN and then tries to access a network resource that relies on Kerberos tickets, the Kerberos Key Distribution Center (KDC) gets the user's information from Active Directory. The KDC uses information from Active Directory to authenticate the user and create a ticket-granting-ticket (TGT). The group membership information in the TGT is up-to-date at the time that the TGT is created.

Windows then uses the TGT to get a session ticket for the requested resource. The session ticket, in turn, uses the group information from the TGT.

The client caches the TGT and continues to use it each time the user starts a new resource session, whether local or on the network. The client also caches the session ticket so that it can continue to connect to the resource (such as when the resource session expires). When the session ticket expires, the client resubmits the TGT for a fresh session ticket.

> **Important**
>
> If the user's group membership changes after the user has started resource sessions, the following factors control when the change actually affects the user's resource access:

- **A change in group membership does not affect existing sessions.**
  Existing sessions continue until either the user signs out or otherwise ends the session, or until the session expires. When a session expires, one of the following things occurs:
  - The client resubmits the session ticket or submits a new session ticket. This operation renews the session.
  - The client does not try to connect again. The session does not renew.
- **A change in group membership does not affect the current TGT, or any session tickets that are created by using that TGT.**
  The ticket granting service (TGS) uses the group information from the TGT to create a session ticket instead of querying Active Directory itself. The TGT isn't renewed until the user locks the client or signs out, or until the TGT expires (typically 10 hours). A TGT can be renewed for 10 days.

You can use the klist command to manually purge a client's ticket cache.

> **Note**
>
> The ticket cache stores tickets for all of the user sessions on the computer. You can use the `klist` command-line options to target the command to specific users or tickets.

Effects on start-up and sign-in processes

The Group Policy service is optimized to speed up the application of group policy and to reduce adverse effects on client performance. For more information, see Understand the Effect of Fast Logon Optimization and Fast Startup on Group Policy. This article provides an in-depth explanation of how Group Policy interacts with start-up and sign-in processes. The Group Policy service can run in the foreground (at startup or sign-in) or in the background (during the user session). The service processes Group Policy in the following manner:

- *Asynchronous processing* refers to processes that do not depend on the outcome of other processes.
- *Synchronous processing* refers to processes that depend on each other's outcome. Therefore, synchronous processes must wait for the previous process to finish before the next process can start.

The following table summarizes the events that trigger foreground or background processing, and whether the processing is synchronous or asynchronous.

Trigger	Synchronous or Asynchronous	Foreground or background
Computer startup or shutdown	Synchronous or asynchronous	Foreground
User sign-in or sign-out	Synchronous or asynchronous	Foreground
Scheduled (during the user session)	Asynchronous	Background
User action (`gpupdate /force`)	Asynchronous	Background

In order to apply configuration changes, some client-side extensions (CSEs) require synchronous processing (at user sign-in or computer startup). In such cases, the CSE identifies the need for a change during background processing. The next time that the user signs in or the computer starts up, the CSE completes the change as part of the synchronous processing phase.

Some of these CSEs have an additional complication: They have to connect to domain controllers or other network servers while the synchronous processing runs. The Folder Redirection and Scripts CSEs are two of the CSEs in this category.

This design works effectively in an office environment. However, in a working-at-home environment, the user might not sign out and back in while connected to the domain. Synchronous processing has to finish before the client contacts a domain controller or any other server. Therefore, some policies cannot be applied or updated correctly.

For example, a change in folder redirection requires all the following:

- Foreground synchronous processing (during user sign-in).
- Connection to a domain controller. The connection must be available while the processing runs.
- Connection to the file server that hosts the redirect target folders. The connection must be available while the processing runs.

In fact, this change can involve two sign-ins. During the first sign-in, the Folder Redirection CSE on the client detects the need for a change and requests the foreground synchronous processing run. During the next sign-in, the CSE implements the policy change.

Effects on Group Policy reporting

The Group Policy service maintains group membership information on the client, in Windows Management Instrumentation (WMI), and in the registry. The WMI store is used in the Resultant Set of Policy report (produced by running `gpresult /r`). It is not used to make decisions about which GPOs are applied.

> **Note**
>
> You can turn off the Resultant Set of Policy reporting function by enabling the **Turn off Resultant Set of Policy logging** policy.

In the following circumstances, the Group Policy service doesn't update the group information in WMI:

- Group Policy is running in the background. For example, during periodic refreshes after the computer has started or a user has signed in, or when a user runs the `gpupdate /force` command to refresh Group Policy.
- Group Policy is running from the Group Policy cache. For example, when the user signs in while the client does not have access to a domain controller.

This behavior means that the group list on a VPN-only client might always be stale because the Group Policy service cannot connect to the network during user sign-in. When Group Policy runs and does not update the group information in WMI, the Group Policy service might record an event that resembles the following:

> GPSVC(231c.2d14) 11:56:10:651 CSessionLogger::Log: restoring old security grps

You can be certain that WMI and the output of `gpresult /r` is updated only when the following line appears in the Group Policy service log for the account that you are examining:

> GPSVC(231c.2d14) 11:56:10:651 CSessionLogger::Log: logging new security grps

Resolution

To resolve the problems that this article describes, use a VPN solution that can establish a VPN connection to a client before the user signs in.

Workarounds

If you cannot use a VPN that establishes a client connection before the user signs in, these workarounds can mitigate the problems that this article describes.

Workaround for user security context and access control

After you add a user to a group or remove a user from a group, provide the following steps to the user. This procedure provides the only supported workaround that refreshes the user security context on clients that do not connect to the VPN before the user signs in.

> **ⓘ Important**
>
> Allow enough time for the membership change to replicate among the domain controllers before you have the user start this procedure.

1. Sign in to the client computer, and then connect to the VPN as you usually do.
2. When you are sure that the client computer is connected to the VPN, lock Windows.
3. Unlock the client computer, and then sign out of Windows.
4. Sign in to Windows again.

The group membership information (and resource access) is now up-to-date.

You can verify the group membership information by opening a Command Prompt window, and then running `whoami /all`.

> **ⓘ Note**
>
> You can use the following Windows PowerShell script to automate the lock and unlock steps of this procedure. In this process, the user has to sign in to Windows, and then has to sign out of Windows after the script runs.

PowerShell

```
$fullname = $env:userdnsdomain + "\" + "$env:username"
$MyCred = Get-Credential -Username $fullname -Message "Update Logon
Credentials"
Start-Process C:\Windows\System32\cmd.exe -ArgumentList ("/C", "exit 0")
-Credential $MyCred -WindowStyle Hidden -PassThru -Wait
```

Workaround for sign-in processes, including Group Policy

You can mitigate some problems by making configuration changes manually, by making script changes so that scripts can run after the user signs in, or by having the user connect to the VPN and then sign out of Windows. You may have to combine these approaches. For Group Policy, in particular, the key is to understand when and how Group Policy can function.

> **Note**
>
> Mapped drive connections and logon scripts do not have the same foreground synchronous processing requirements as folder redirections, but they do require domain controller and resource server connectivity.

For a detailed list of the processing requirements of Group Policy CSEs, see Understand the Effect of Fast Logon Optimization and Fast Startup on Group Policy.

Group Policy is not applied to a user account for RunAs.exe or "Run as different user"

Article • 09/23/2021 • 2 minutes to read

This article provides some information for the issue where Group Policy is not applied to a user account for RunAs.exe or "Run as different user".

Applies to: Windows 10 - all editions
Original KB number: 4569309

Summary

A Windows user can run a program or application as a different user. To do this, the user selects the **Run as different user** context menu command (or uses the Runas.exe command-line tool), and then specifies the credentials of an alternate account.

As a best practice, users should do their usual work on their workstations by using their own credentials. They can specify the credentials of an alternate account (such as an account that has elevated permissions) to run a specific application, as necessary.

However, when a user signs in by using alternate credentials, Windows does not process Group Policy settings for the alternate account. Windows processes Group Policy settings for a user account only if the user signs in to their own desktop by using the sign-in user interface. By contrast, when a user starts an application by using Runas.exe or **Run as different user**, Windows starts a separate process that runs under the alternate credentials. Such an operation does not trigger Group Policy processing.

This behavior is by design.

More information

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

Group Policy settings are not intended to apply to the alternate user account that is specified by Runas.exe or **Run as different user**.

Runas.exe can load the user profile that is associated with the alternate account. If a user previously signed in to Windows on that workstation by using that account, the associated user profile might contain registry keys and values that were set by Group Policy processing events at that time. However, this behavior depends on whether the user includes the `/noprofile` switch in the command. If the user starts a process or application by using `runas /noprofile`, and then specifies the alternate account, Windows does not load the alternate user profile. Therefore, the alternate user profile does not provide a reliable way to apply Group Policy settings.

If you want to prevent users from using Runas.exe or **Run as different user**, follow these steps.

> **ⓘ Important**
>
> After you apply these settings, any functionality that depends on the "Run as" feature does not work.

1. Disable the **Secondary Logon** service (seclogon.exe).
2. Use Software Restriction Policies or AppLocker to prevent access to the Runas.exe binary file.
3. Use Group Policy to remove the **Run as different user** menu item. The Group Policy Object (GPO) changes to User Configuration\Administrative Templates\Start Menu and Taskbar\Show "Run as different user" command on Start.
4. In the Windows registry, set the following entry:
    - Subkey: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\`
    - Entry name: HideRunAsVerb
    - Type: DWORD
    - Value: 1

Group Policy Screensaver setting isn't working in Windows

Article • 09/23/2021 • 2 minutes to read

This article helps work around an issue where the Screensaver doesn't start after a Group Policy is configured to enable it in Windows.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2616727

Symptoms

A Group Policy is configured to enable Screensaver:

User Configuration\Administrative Templates\Control Panel\Personalization\Enable screen saver

But there's no setting defining a ScreenSaverTimeout configured in Screen saver timeout.

The Screensaver won't start in such a configuration by default.

Cause

The default ScreenSaver Timeout is configured in the registry at this location:

- Registry subkey: `HKEY_CURRENT_USER\Control Panel\Desktop`
- Type: Reg_SZ
- Name: ScreenSaveTimeOut

Since Windows 7/Windows Server 2008 R2, this key doesn't exist by default.

Without configuring a default timeout via Group Policy, the system doesn't have a timeout and therefore doesn't start the screensaver.

Workaround

There are two workarounds to solve this issue.

- Configure the **Screen saver timeout** Group Policy under the following path to change the default ScreenSaver timeout:

User Configuration\Administrative Templates\Control Panel\Personalization\

- Use Group Policy Preferences to configure a new default value for the following registry key in a Group Policy applying to users:
  - Registry subkey: `HKEY_CURRENT_USER\Control Panel\Desktop`
  - Type: Reg_SZ
  - Name: ScreenSaveTimeOut

    User Configuration > Preferences > Windows Settings > Registry

    New > Registry Item
  - Action: Create
  - Hive: `HKEY_CURRENT_USER`
  - Key Path: `Control Panel\Desktop`
  - Value Name: ScreenSaveTimeOut
  - Value Type: REG_SZ
  - Value Data: 600

    Using Item Level Targeting (Common Tab of setting) the appliance of this setting can be restricted to systems running Windows 7 or Windows Server 2008 R2.

Point and Print Restrictions policies are ignored in Windows

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where the Point and Print Restrictions policies are ignored when a standard user tries to install a network printer.

Applies to: Windows Server 2012 R2, Windows 7 Service Pack 1
Original KB number: 2307161

Symptoms

Consider the following scenario:

- You have a computer that is running Windows.
- You apply the Point and Print Restrictions policies.
- A standard user tries to install a network printer.

In this scenario, the Point and Print Restrictions policies are ignored, and the user is prompted for administrative credentials.

Cause

Windows ignore the Point and Print Restrictions policies when the policies are implemented in the user policy context.

The Point and Print Restrictions policies were previously implemented in the following location:

User Configuration\Policies\Administrative Templates\Control Panel\Printers

Now, these policies are implemented in the following location:

Computer Configuration\Policies\Administrative Templates\Printers: Point and Print Restrictions

To have a consistent experience, we recommend that you set the policy in both locations if you're dealing with mixed-level clients.

Resolution

> **Note**
>
> The following procedure assumes that you're using the version of the Group Policy Management Console (GPMC) that is included with Windows. Otherwise, you must have updated ADMX files in your domain central store in order to see these options. To install the GPMC on Windows, use the Add Features Wizard of Server Manager.

How to change the Point and Print Restrictions policies setting

1. Open the Group Policy Management Console (GPMC).
2. In the GPMC console tree, navigate to the domain or organizational unit (OU) that stores the user accounts for which you want to modify printer driver security settings.
3. Right-click the appropriate domain or OU, click **Create a GPO in this domain, and Link it here**, type a name for the new GPO, and then click **OK**.
4. Right-click the GPO that you created, and then click **Edit**.
5. In the Group Policy Management Editor window, click **Computer Configuration**, click **Policies**, click **Administrative Templates**, and then click **Printers**.
6. Right-click **Point and Print Restrictions**, and then click **Edit**.

How to permit users to connect only to specific print servers that you trust

1. In the **Point and Print Restrictions** dialog box, click **Enabled**.

   Computer Configuration\Policies\Administrative Templates\Printers: Point and Print Restrictions

   Setting: Enabled

2. Click to select the Users can only point and print to these servers check box if it's not already selected.

3. In the text box, type the fully qualified server names to which you want to allow users to connect. Separate each name by using a semicolon (;).

4. In the **When installing drivers for a new connection** box, select **Do not show warning or elevation prompt**.

5. In the **When updating drivers for an existing connection** box, select **Show warning only**.
6. Click **OK**.

More information

Alternatively, you can disable the driver installation warning messages and elevation prompts by completely disabling the Point and Print Restrictions policies. This action disables the enhanced printer driver installation security.

Computer Configuration\Policies\Administrative Templates\Printers: Point and Print Restrictions

Setting: Disable

Save documents to OneDrive by default is a OneDrive Group Policy Administrative Templates discrepancy in Windows 8.1

Article • 09/23/2021 • 2 minutes to read

This article explains a discrepancy in the policy name in Microsoft OneDrive Group Policy Administrative Templates.

Applies to: Windows 8.1
Original KB number: 3017037

Symptoms

In the OneDrive Group Policy Administrative Templates that are dated September 12, 2014, there is a discrepancy in the policy name and description for where you can save documents by default.

More information

Currently, the inaccurate policy name is: **Save documents to OneDrive by default**.

And the policy description is as follows:

This policy setting lets you disable OneDrive as the default save location. It does not prevent apps and users from saving files on OneDrive. If you disable this policy setting, files will be saved locally by default. Users will still be able to change the value of this setting to save to OneDrive by default. They will also be able to open and save files on OneDrive using the OneDrive app and file picker, and Microsoft Store apps will still be able to access OneDrive using the WinRT API. If you enable or do not configure this policy setting, users with a connected account will save documents to OneDrive by default.

Actually, the policy name should be: **Save documents to the local PC by default**

And the policy description should read: This policy setting lets you select the local PC as the default save location. It does not prevent apps and users from saving files on OneDrive. If you enable this policy setting files will be saved locally by default. Users will still be able to change the value of this setting to save to OneDrive by default. They will

also be able to open and save files on OneDrive using the OneDrive app and file picker and Microsoft Store apps will still be able to access OneDrive using the WinRT API. If you disable or do not configure this policy setting, users with a connected account will save files to OneDrive by default.

How to use Group Policy to deploy a Known Issue Rollback

Article • 08/02/2022 • 13 minutes to read

This article describes how to configure Group Policy to use a Known Issue Rollback (KIR) policy definition that activates a KIR on managed devices.

Applies to: Windows Server 2019, version 1809 and later versions; Windows 10, version 1809 and later versions

Summary

Microsoft has developed a new Windows servicing technology that's named KIR for Windows Server 2019 and Windows 10, versions 1809 and later versions. For the supported versions of Windows, a KIR rolls back a specific change that was applied as part of a nonsecurity Windows Update release. All other changes that were made as a part of that release remain intact. By using this technology, if a Windows update causes a regression or other problem, you don't have to uninstall the entire update and return the system to the last known good configuration. You roll back only the change that caused the problem. This rollback is temporary. After Microsoft releases a new update that fixes the problem, the rollback is no longer necessary.

> **Important**
>
> KIRs apply to only nonsecurity updates. This is because rolling back a fix for a nonsecurity update doesn't create a potential security vulnerability.

Microsoft manages the KIR deployment process for non-enterprise devices. For enterprise devices, Microsoft provides KIR policy definition MSI files. Enterprises can then use Group Policy to deploy KIRs in hybrid Azure Active Directory (Azure AD) or Active Directory Domain Services (AD DS) domains.

> **Note**
>
> You have to restart the affected computers in order to apply this Group Policy change.

The KIR process

If Microsoft determines that a nonsecurity update has a critical regression or similar issue, Microsoft generates a KIR. Microsoft announces the KIR in the Windows Health Dashboard, and adds the information to the following locations:

- The Known Issues section of the applicable Windows Update KB article
- The Known Issues list on the Windows Health Release Dashboard at https://aka.ms/windowsreleasehealth for the affected versions of Windows (for example, Windows 10, version 20H2 and Windows Server, version 20H2)

For non-enterprise customers, the Windows Update process applies the KIR automatically. No user action is required.

For enterprise customers, Microsoft provides a policy definition MSI file. Enterprise customers can propagate the KIR to managed systems by using the enterprise Group Policy infrastructure.

To see an example of a KIR MSI file, download Windows 10 (2004 & 20H2) Known Issue Rollback 031321 01.msi.

A KIR policy definition has a limited lifespan (a few months, at most). After Microsoft publishes an amended update to address the original issue, the KIR is no longer necessary. The policy definition can then be removed from the Group Policy infrastructure.

Apply KIR to a single device using Group Policy

To use Group Policy to apply a KIR to a single device, follow these steps:

1. Download the KIR policy definition MSI file to the device.

   > **Important**
   >
   > Make sure that the operating system that is listed in the .msi file name matches the operating system of the device that you want to update.

2. Run the .msi file on the device. This action installs the KIR policy definition in the Administrative Template.
3. Open the Local Group Policy Editor. To do this, select **Start**, and then enter *gpedit.msc*.
4. Select **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **KB ####### Issue *XXX* Rollback** > **Windows 10, version *YYMM***.

> **Note**
>
> In this step, ####### is the KB article number of the update that caused the problem. *XXX* is the issue number, and *YYMM* is the Windows 10 version number.

5. Right-click the policy, and then select **Edit** > **Disabled** > **OK**.
6. Restart the device.

For more information about how to use the Local Group Policy Editor, see Working with the Administrative Template policy settings using the Local Group Policy Editor.

Apply a KIR to devices in a hybrid Azure AD or AD DS domain using Group Policy

To apply a KIR policy definition to devices that belong to a hybrid Azure AD or AD DS domain, follow these steps:

1. Download and install the KIR MSI files
2. Create a Group Policy Object (GPO).
3. Create and configure a WMI filter that applies the GPO.
4. Link the GPO and the WMI filter.
5. Configure the GPO.
6. Monitor the GPO results.

1. Download and install the KIR MSI files

1. Check the KIR release information or the known issues lists to identify which operating system versions you have to update.
2. Download the KIR policy definition .msi files that you require to update to the computer that you use to manage Group Policy for your domain.
3. Run the .msi files. This action installs the KIR policy definition in the Administrative Template.

> **Note**
>
> Policy definitions are installed in the *C:\Windows\PolicyDefinitions* folder. If you have implemented the Group Policy **Central Store**, you must copy the .admx and .adml files to the Central Store.

2. Create a GPO

1. Open Group Policy Management Console, and then select **Forest: *DomainName*** > **Domains**.
2. Right-click your domain name, and then select **Create a GPO in this domain, and link it here**.
3. Enter the name of the new GPO (for example, **KIR Issue *XXX***), and then select **OK**.

For more information about how to create GPOs, see Create a Group Policy Object.

3. Create and configure a WMI filter that applies the GPO

1. Right-click **WMI Filters**, and then select **New**.
2. Enter a name for your new WMI filter.
3. Enter a description of your WMI filter, such as **Filter to all Windows 10, version 2004 devices**.
4. Select **Add**.
5. In **Query**, enter the following query string:

```
SQL

SELECT version, producttype from Win32_OperatingSystem WHERE Version =
<VersionNumber>
```

> **ⓘ Important**
>
> In this string, <VersionNumber> represents the Windows version that you want the GPO to apply to. The version number must use the following format (exclude the brackets when you use the number in the string):
>
> > 10.0.*xxxxx*
>
> where *xxxxx* is a five digit number. Currently, KIRs support the following versions:

Version	Build number
Windows 10, version 20H2	10.0.19042
Windows 10, version 2004	10.0.19041

Version	Build number
Windows 10, version 1909	10.0.18363
Windows 10, version 1903	10.0.18362
Windows 10, version 1809	10.0.17763

For an up-to-date list of Windows releases and build numbers, see Windows 10 - release information.

> **Important**
>
> The build numbers that are listed on the Windows 10 release information page don't include the **10.0** prefix. To use a build number in the query, you must add the **10.0** prefix.

For more information about how to create WMI filters, see Create WMI Filters for the GPO.

4. Link the GPO and the WMI filter

1. Select the GPO that you created previously, open the **WMI Filtering** menu, and then select the WMI filter that you just created.
2. Select **Yes** to accept the filter.

5. Configure the GPO

Edit your GPO to use the KIR activation policy:

1. Right-click the GPO that you created previously, and then select **Edit**.
2. In the Group Policy Editor, select ***GPOName*** > **Computer Configuration** > **Administrative Templates** > **KB ####### Issue *XXX* Rollback** > **Windows 10, version *YYMM***.
3. Right-click the policy, and then select **Edit** > **Disabled** > **OK**.

For more information about how to edit GPOs, see Edit a Group Policy object from GPMC.

6. Monitor the GPO results

In the default configuration of Group Policy, managed devices should apply the new policy within 90 to 120 minutes. To speed up this process, you can run `gpupdate` on affected devices to manually check for updated policies.

Make sure that each affected device restarts after it applies the policy.

> **Important**
>
> The fix that introduced the issue is disabled after the device applies the policy and then restarts.

Deploy a KIR activation using Microsoft Intune ADMX policy ingestion to the managed devices

> **Note**
>
> To use the solutions in this section, you must install the cumulative update that is released on **July 26, 2022** or a later one on the computer.

Group Policies and GPOs aren't compatible with mobile device management (MDM) based solutions, such as Microsoft Intune. These instructions will guide you through how to use Intune custom settings for ADMX ingestion and configure ADMX backed MDM policies to perform a KIR activation without requiring a GPO.

To perform a KIR activation on Intune managed devices, follow these steps:

1. Download and install the KIR MSI file to get ADMX files.
2. Create a custom configuration profile in Microsoft Endpoint Manager.
3. Monitor KIR activation.

1. Download and install the KIR MSI file to get ADMX files

1. Check the KIR release information or the known issues lists to identify which operating system (OS) versions you must update.

2. Download the required KIR policy definition .msi files on the machine you use to sign in to Microsoft Endpoint Manager.

   > **Note**

You will need access to the contents of a KIR activation ADMX file.

3. Run the `.msi` files. This action installs the KIR policy definition in the Administrative Template.

> **Note**
>
> Policy definitions are installed in the *C:\Windows\PolicyDefinitions* folder.
>
> If you want to extract the ADMX files to another location, use the `msiexec` command with the **TARGETDIR** property. For example:

```
Console

msiexec /i c:\admx_file.msi /qb TARGETDIR=c:\temp\admx
```

2. Create a custom configuration profile in Microsoft Endpoint Manager

To configure devices to perform a KIR activation, you need to create a custom configuration profile for each OS of your managed devices. To create a custom profile, follow these steps:

1. Select properties and add basic information of the profile.
2. Add custom configuration setting to ingest ADMX files for KIR activation.
3. Add custom configuration setting to set new KIR activation policy.
4. Assign devices to the KIR activation custom configuration profile.
5. Use applicability rules to target devices to receive KIR custom configuration settings by OS.
6. Review and create KIR activation custom configuration profile.

A. Select properties and add basic information about the profile

1. Sign in to the Microsoft Endpoint Manager admin center.
2. Select **Devices** > **Configuration profiles** > **Create profile**.
3. Select the following properties:
   - **Platform**: **Windows 10 and later**
   - **Profile**: **Templates** > **Custom**

4. Select **Create**.

5. In **Basics**, enter the following properties:

   - **Name**: Enter a descriptive name for the policy. Name your policies so you can easily identify them later. For example, a good policy name is "04/30 KIR Activation – Windows 10 21H2".
   - **Description**: Enter a description for the policy. This setting is optional but recommended.

   > ⓘ Note
   >
   > **Platform** and **Profile type** should already have values selected.

6. Select **Next**.

> ⓘ Note
>
> For more information about creating custom configuration profiles and configuration settings, see **Use custom device settings in Microsoft Intune**.

Before proceeding to the next two steps, open the ADMX file in a text editor (for example, Notepad) where the file was extracted. The ADMX file should be in the path *C:\Windows\PolicyDefinitions* if you installed it as an MSI file.

Here's an example of the ADMX file:

XML

```
<policies>
  <policy name="KB5011563_220428_2000_1_KnownIssueRollback" … >
    <parentCategory ref="KnownIssueRollback_Win_11" />
    <supportedOn ref="SUPPORTED_Windows_11_0_Only" />
    <enabledList…> … </enabledList>
    <disabledList…>…</disabledList>
  </policy>
</policies>
```

Record the values for `policy name` and `parentCategory`. This information is in the "policies" node at the end of the file.

B. Add custom configuration setting to ingest ADMX files for KIR activation

This configuration setting is used to install the KIR activation policy on target devices. Follow these steps to add the ADMX ingestion settings:

1. In **Configuration settings**, select **Add**.
2. Enter the following properties:
    - **Name**: Enter a descriptive name for the configuration setting. Name your settings so you can easily identify them later. For example, a good setting name is "ADMX Ingestion: 04/30 KIR Activation – Windows 10 21H2".
    - **Description**: Enter a description for the setting. This setting is optional but recommended.
    - **OMA-URI**: Enter the string *./Device/Vendor/MSFT/Policy/ConfigOperations/ADMXInstall/KIR/Policy/<ADMX Policy Name>*.

      > ⓘ **Note**
      >
      > Replace <ADMX Policy Name> with the value of the recorded policy name from the ADMX file. For example, "KB5011563_220428_2000_1_KnownIssueRollback".

    - **Data type**: Select **String**.
    - **Value**: Open the ADMX file with a text editor (for example, Notepad). Copy and paste the entire contents of the ADMX file you intend to ingest into this field.
3. Select **Save**.

C. Add custom configuration setting to set new KIR activation policy

This configuration setting is used to configure the KIR activation policy, which is defined in the previous step.

Follow these steps to add the KIR activation configuration settings:

1. In **Configuration settings**, select **Add**.
2. Enter the following properties:

- **Name**: Enter a descriptive name for the configuration setting. Name your settings so you can easily identify them later. For example, a good setting name is "KIR Activation: 04/30 KIR Activation – Windows 10 21H2".
- **Description**: Enter a description for the setting. This setting is optional but recommended.
- **OMA-URI**: Enter the string *./Device/Vendor/MSFT/Policy/Config/KIR~Policy~KnownIssueRollback~<Parent Category>/<ADMX Policy Name>*.

  > ⓘ **Note**
  >
  > Replace <Parent Category> with the parent category string recorded in the previous step. For example, "KnownIssueRollback_Win_11". Replace <ADMX Policy Name> with the same policy name used in the previous step.

- **Data type**: Select **String**.
- **Value**: Enter *<disabled/>*.

3. Select **Save**.
4. Select **Next**.

D. Assign devices to the KIR activation custom configuration profile

After you've defined what the custom configuration profile does, follow these steps to identify which devices you'll configure:

1. In **Assignments**, select **Add all devices**.
2. Select **Next**.

E. Use applicability rules to target devices to receive KIR custom configuration settings by OS

To target the devices by OS that are applicable to the GP, add an applicability rule to check the device OS Version (Build) before applying this configuration. You can look up the build numbers for the supported OS on the following pages:

- Windows 11 release information
- Windows 10 release information

- Windows Server release information

The build numbers shown in the pages are formatted as MMMMM.mmmm (M= major version and m= minor version). The OS Version properties use the major version digits. The OS Version values entered into the Applicability Rules should be formatted as "10.0.MMMMM". For example, "10.0.22000".

Follow these instructions to set the correct Applicability Rules for your KIR activation:

1. In **Applicability Rules**, create an applicability rule by entering the following properties on the blank rule already on the page:

    - **Rule**: Select **Assign profile if** from the dropdown list.
    - **Property**: Select **OS Version** from the dropdown list.
    - **Value**: Enter the Min and the Max OS version numbers formatted as "10.0.MMMMM".

2. Select **Next**.

> ⓘ **Note**
>
> The OS version of a device can be found by running the `winver` command from the Start menu. It will show a two-part version number separated by a ".". For example, "22000.613". You can append the left number to "10.0." for the Min OS version. Obtain the Max OS version number by adding 1 to the last digit of the Min OS version number. For this example, you can use these values:
> Min OS version: "10.0.22000"
> Max OS version: "10.0.22001"

F. Review and create KIR activation custom configuration profile

Review your settings of the custom configuration profile and select **Create**.

3. Monitor KIR activation

Your KIR activation should be in progress now. Follow these steps to monitor the configuration profile progress:

1. Go to **Devices** > **Configuration profiles**, and select an existing profile. For example, select a macOS profile.

2. Select the **Overview** tab. In this view, the **Profile assignment status** includes the following statuses:

    - **Succeeded**: Policy is applied successfully.
    - **Error**: The policy failed to apply. The message typically displays an error code that links to an explanation.
    - **Conflict**: Two settings are applied to the same device, and Intune can't sort out the conflict. An administrator should review the conflict.
    - **Pending**: The device hasn't checked in with Intune to receive the policy yet.
    - **Not applicable**: The device can't receive the policy. For example, the policy updates a setting specific to iOS 11.1, but the device is using iOS 10.

For more information, see Monitor device configuration profiles in Microsoft Intune.

More information

- Local Group Policy Editor
- Working with the Administrative Template policy settings using the Local Group Policy Editor
- Group Policy Overview
- GPMC How To
- Create WMI Filters for the GPO (Windows 10) - Windows security
- Edit a Group Policy object from GPMC
- Create and manage group policy in Azure AD Domain Services
- Use Windows 10/11 templates to configure group policy settings in Microsoft Intune

High Availability troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve High Availability-related issues. Browse the content or use the search feature to find relevant content.

High Availability sub category

- Nested Virtualization

How to retrieve data from a Windows XP Mode virtual machine on Windows 8 or Windows 10

Article • 11/18/2022 • 2 minutes to read

This article provides methods to retrieve data from a Windows XP Mode virtual machine in Windows 10.

Applies to: Windows 10 - all editions
Original KB number: 2724115

Summary

With the end of extended support for Windows XP in April 2014, Microsoft has decided not to develop Windows XP Mode for Windows 8 and above. If you're a Windows 7 customer who uses Windows XP Mode and are planning a move to Windows 10, this article may be helpful to you.

When you upgrade from Windows 7 to Windows 10, Windows XP Mode is installed on your machine, however Windows Virtual PC isn't present anymore. This issue occurs because Windows Virtual PC isn't supported on Windows 8 and above. To retrieve data from the Windows XP Mode virtual machine, use one of the following methods.

Method 1

Mount the virtual hard disk that was attached to the Windows XP Mode virtual machine, and then extract the data from the mounted drive.

1. On the Windows 10 machine, locate your Windows XP Mode virtual hard disk. The default location is: %LocalAppData%/Microsoft/Windows Virtual PC/Virtual Machines/Windows XP Mode.vhd.
2. Right-click the virtual hard disk, and then select **Mount**.
3. The contents of the virtual hard disk will appear as a local drive on the Windows PC (for example, G:\).
4. Locate data that needs to be extracted, and copy the data to another location.
5. To unmount the virtual hard disk, right-click the new local drive (for example, G:\), and then select **Eject**.
6. Uninstall Windows XP Mode when all data has been retrieved.

Method 2

Copy the Windows XP Mode virtual hard disks to another Windows 7 machine, and use Windows Virtual PC to run the virtual machine. Then extract the data from the virtual machine.

1. Copy your Windows XP Mode virtual hard disk (Default location: %LocalAppData%/Microsoft/Windows Virtual PC/Virtual Machines/Windows XP Mode.vhd), and the base virtual hard disk (default location: %ProgramFiles%\Windows XP Mode\Windows XP Mode base.vhd) from the Windows 10 PC to another Windows 7 PC.

2. Ensure the base disk is copied to the exact same location as it existed on the previous Windows 7 PC (for example, C:\Program Files\Windows XP Mode\Windows XP Mode base.vhd).

3. Create a new virtual machine with Windows Virtual PC. Then point to your Windows XP Mode virtual hard disk as the disk for the new virtual machine.

4. Start the virtual machine, login, and copy any required data from the virtual machine to another location.

5. Delete the virtual machine, and uninstall Windows XP Mode when all data is retrieved.

> **Note**
>
> The Windows XP Mode virtual hard disk will not work on Windows 8 and above as they does not provide the Windows XP Mode license. The Windows XP Mode license is a benefit provided on Windows 7 only.

Windows clients networking troubleshooting documentation

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Networking-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Networking sub categories

- Access to remote file shares (SMB or DFS Namespace)
- DNS
- Dynamic Host Configuration Protocol (DHCP)
- Folder redirection and Offline Files and Folders (CSC)
- IP Address Management (IPAM)
- Remote access
- TCP/IP communications
- Web Application Proxy (WAP) role service
- WebClient and WebDAV
- Windows Defender Exploit Guard
- Windows Firewall with Advanced Security (WFAS)
- Wireless networking and 802.1X authentication

Error when you try to access a network drive that's mapped to a web share: User has not been authenticated

Article • 09/23/2021 • 5 minutes to read

This article provides a resolution for an issue that occurs on a Windows-based computer when you try to access a mapped web share.

Applies to: Windows 10 – all editions, Windows 7 Service Pack 1
Original KB number: 941050

Symptoms

Consider the following scenario on a Windows-based computer:

- You map a network drive to a web share that requires user credentials.
- You configure the drive to use the **Reconnect at logon** option.
- You enter the user credentials, and then you select the **Remember my password** check box when you access the drive.
- You restart the computer, or you log off from Windows.

In this scenario, when you log on to the computer again, you receive an error message that resembles the following when you try to access the mapped drive:

> An error occurred while connecting to **address**
> The operation being requested was not performed because the user has not been authenticated
> The connection has not been restored

> **Note**
>
> The mapped drive appears as disconnected after you log on to the computer again.

Cause

This issue occurs because the Web Distributed Authoring and Versioning (WebDAV) redirector uses Windows HTTP Services (WinHTTP) instead of the Windows Internet (WinInet) API. In a non-proxy network configuration, WinHTTP sends user credentials

only in response to requests that occur on a local intranet site. Therefore, if no proxy is configured, you may be unable to access a share that requires user credentials.

Resolution

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:
> 322756 How to back up and restore the registry in Windows

To resolve this problem in Windows Vista, apply hotfix 943280. The hotfix is only for Windows Vista. For later versions of Windows, go to the next section to modify the registry keys.

> **Note**
>
> This hotfix applies only to Windows Vista-based systems. However, the registry changes described later in this section apply to all the operating systems in the "Applies To" section. No hotfix is required for systems that are running Windows 7, Windows 8.1, or Windows 10. The registry changes alone fix the problem on these systems.

For more information, click the following article number to view the article in the Microsoft Knowledge Base:

943280 You are prompted to enter your credentials when you access an FQDN site by using a Windows Vista-based client computer that has no proxy configured

After you apply this hotfix, you must create a registry entry. To do this, follow these steps:

1. Click **Start**, type *regedit* in the **Start Search** box, and then press Enter.
2. Locate and then click the following subkey:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters`

3. On the **Edit** menu, point to **New**, and then click **Multi-String Value**.
4. Type **AuthForwardServerList**, and then press Enter.
5. On the **Edit** menu, click **Modify**.
6. In the **Value date** box, type the URL of the server that hosts the web share, and then click **OK**.

   > ⓘ **Note**
   >
   > You can also type a list of URLs in the **Value date** box. For more information, see the "Sample URL list" section.

7. Exit Registry Editor.

After this registry entry is created, the WebClient service will read the entry value. If the client computer tries to access a URL that matches any of the expressions in the list, the user credential will be successfully sent to authenticate the user even if no proxy is configured.

> ⓘ **Note**
>
> You must restart the WebClient service after you modify the registry.

Sample URL list

The following is a sample URL list:

`https://*.Contoso.com`

`http://*.dns.live.com`

`*.microsoft.com`

`https://172.169.4.6`

This URL list enables the WebClient service to send credentials through the following channels.

> ⓘ **Note**

After you configure this URL list, the credentials will automatically authenticate to the WebDAV servers even if these servers are on the Internet.

- Any encrypted channel to a child domain of a domain whose name is `Contoso.com`.
- Any nonsecure channel to a child domain of a domain whose name is `dns.live.com`.
- Any channel to a server whose name ends with ".microsoft.com."
- Any encrypted channel to a host whose IP address is 172.169.4.6.

Things to avoid in the URL list

- Don't add an asterisk (*) at the end of a URL. When you do this, a security risk may result. For example, don't use the following:

  `http://*.dns.live.*`

- Don't add an asterisk (*) before or after a string. When you do this, the WebClient service can send user credentials to more servers. For example, don't use the following:
  - `http://Contoso.com`

  In this example, the service also sends user credentials to `http://**extra_characters** Contoso.com`.
  - `http://Contoso*.com`

  In this example, the service also sends user credentials to `http://Contoso **extra_characters**.com`.

- Don't type the UNC name of a host in the URL list. For example, don't use the following:

  `*.contoso.com@SSL`

- Don't include the share name or the port number to be used in the URL list. For example, don't use the following:
  - `http://*.dns.live.com/DavShare`
  - `http://*dns.live.com:80`

- Don't use IPv6 in the URL list.

> **Important**
>
> This URL list has no effect on the security zone settings, and this URL list is used only for the specific purpose of forwarding the credentials to WebDAV servers. Create the list as restrictively as possible to avoid any security issues. Also, notice that there is no specific deny list. Therefore, the credentials are forwarded to all the servers that match this list.

If Basic authentication or Digest authentication is implemented in the network, hotfix 943280 can't change this behavior. This behavior is by design in Basic authentication mode and in Digest authentication mode.

IIS doesn't support Windows authentication over the Internet. Therefore, this hotfix applies only to the Intranet scenarios.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the "Applies to" section.

Access Denied when you access an SMB file share in Windows

Article • 09/23/2021 • 2 minutes to read

This article helps fix the **Access Denied** error that occurs when you access a Server Message Block (SMB) file share.

Applies to: Windows Server 2012 R2, Windows 7 Service Pack 1
Original KB number: 3035936

Symptoms

When you try to access a specific folder that's located on a Network Appliance (NetApp) Filer or a Windows Server that supports SMB2 from a Windows-based system through the SMB Version 2 protocol, the access is denied. This issue occurs in the following version of Windows:

- Windows 8.1
- Windows Server 2012 R2
- Windows 8
- Windows Server 2012
- Windows 7
- Windows Server 2008 R2
- Windows Vista
- Windows Server 2008

> **Note**
>
> This issue doesn't occur if you disable the SMB2 protocol on the client or use a Windows SMB client, such as Windows XP or Windows Server 2003.

Cause

This issue occurs because the target folder on the SMB share is missing the SYNCHRONIZE access control entries.

Resolution

To resolve this issue, use the ICACLS utility to set the desired permissions that contain the Synchronize bit.

For example, at a command prompt, type the following command, and then press ENTER:

Console

```
ICACLS h:\folder /grant domain\user:(RC,RD,REA,RA,X,S)
```

A comma-separated list in parentheses of specific rights:

- RC - read control
- RD - read data/list directory
- REA - read extended attributes
- RA - read attributes
- X - execute/traverse
- S - Synchronize

Troubleshooting

You can use the following methods to verify and troubleshoot the issue.

1. Verify that the NetApp Filer has the Synchronize bit set on the folder.
2. A network trace can show the **DesiredAccess** error for the SMB2 CREATE process on the folder for the Request and Response packet.
3. The AccessChk.exe tool is available on Windows Sysinternals site for reading out the permission settings.

   For example, run the following command:

   Console

   ```
   C:\tools\Sysinternals\accesschk.exe -ld
   ```

   Then, you can see the following result that shows the SYNCHRONIZE bit is set:

   Output

   ```
   [2] ACCESS_ALLOWED_ACE_TYPE: BUILTIN\Users
   [OBJECT_INHERIT_ACE]
   [CONTAINER_INHERIT_ACE]
   [INHERITED_ACE]
   ```

```
FILE_LIST_DIRECTORY
FILE_READ_ATTRIBUTES
FILE_READ_EA
FILE_TRAVERSE
SYNCHRONIZE
READ_CONTROL
```

See the behavior of the SYNCHRONIZE bit on Windows SMB2 clients.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

You can still access offline files even though the file server is removed from the network on a Windows 7-based client computer

Article • 09/23/2021 • 2 minutes to read

This article describes an issue where you can still access offline files even though the file server is removed from the network.

Applies to: Windows 7 Service Pack 1
Original KB number: 942974

Symptoms

On a Windows Vista-based or Windows 7-based client computer, you can still access offline files even though the file server is removed from the network. Additionally, you can delete the offline files and the temporary files in the **Offline Files** item in Control Panel.

Resolution

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:
> 322756 How to back up and restore the registry in Windows

To resolve this problem, reinitialize the cache of offline files. To do this, follow these steps:

1. Click **Start**, type *regedit* in the **Start Search** box, and then press Enter.

> **Note**
>
> If you are prompted for an administrator password or for confirmation, type the password or click **Continue**.

2. Locate the following registry subkey, and then right-click it:

   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CSC`

3. Point to **New**, and then click **Key**.
4. Type *Parameters* in the box.
5. Right-click **Parameters**, point to **New**, and then click **DWORD (32-bit) Value**.
6. Type *FormatDatabase*, and then press Enter.
7. Right-click **FormatDatabase**, and then click **Modify**.
8. In the **Value data** box, type *1*, and then click **OK**.
9. Exit Registry Editor, and then restart the computer.

> **Note**
>
> Make sure that files are synchronized before you add this registry entry. Otherwise, unsynchronized changes will be lost.

You can also automate the process of setting this registry value by using the Reg.exe command line tool. To do this, run the following command from an administrative command prompt:

Console

```
REG ADD "HKLM\System\CurrentControlSet\Services\CSC\Parameters" /v
FormatDatabase /t REG_DWORD /d 1 /f
```

> **Note**
>
> - Make sure that files are synchronized before you add this registry entry. Otherwise, unsynchronized changes will be lost.
> - The actual value of the new registry key is ignored.

- This registry change requires a restart. When the computer is restarting, the shell will re-initialize the CSC cache, and then delete the registry key if the registry entry exists.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the "Applies to" section.

Can't access shared folders from File Explorer in Windows 10

Article • 03/09/2022 • 3 minutes to read

Applies to: Windows 10

General troubleshooting

- Instead of **File Explorer**, access the shared folder by **Command Prompt** using the below command:

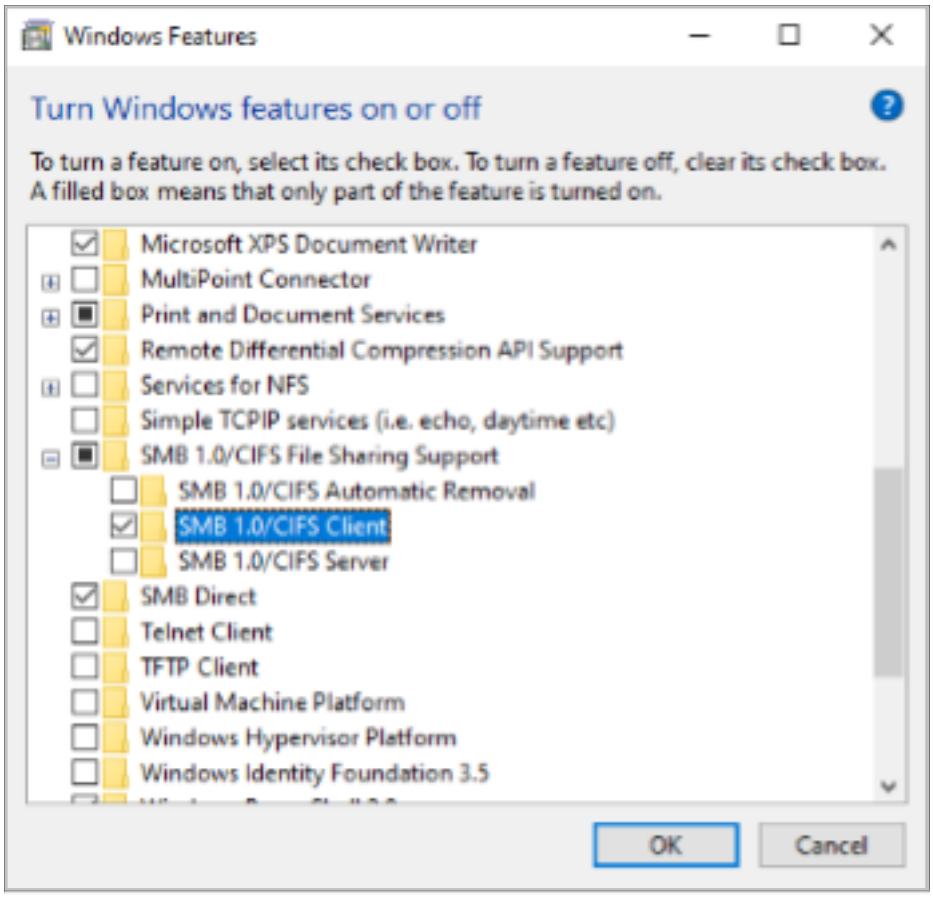
  ```
  Console

  net use <DeviceName>: \\<ServerName>\<ShareName>
  ```

  > **Note**
  >
  > For more information, see **Net use**.

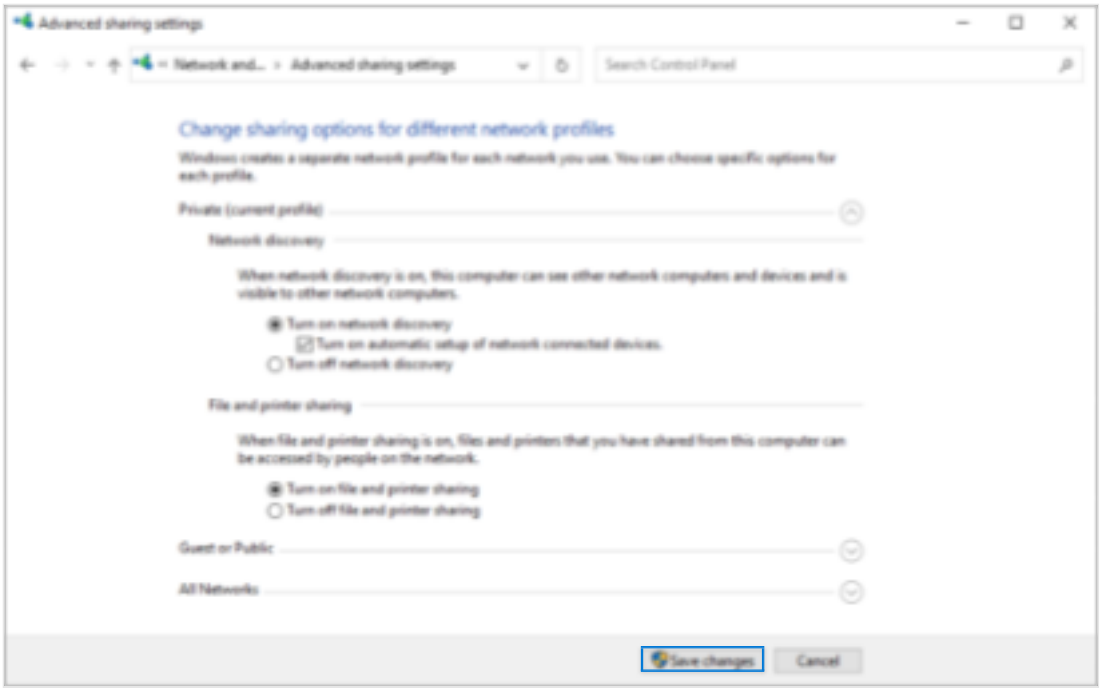
- Turn on the SMB 1.0 support feature from **Control Panel** by following these steps:

  1. Open **Control Panel**.
  2. Select **Programs** > **Programs and Features** > **Turn Windows features on or off** > **SMB 1.0/CIFS File Sharing Support**.
  3. Check **SMB 1.0/CIFS Client**, and then press Enter.



- Turn on network discovery and file and printer sharing options by following these steps:

    1. Open **Control Panel**.
    2. Select **Network and Internet** > **Network and Sharing Center** > **Advanced sharing settings**.
    3. Select **Turn on network discovery**.
    4. Select **Turn on file and printer sharing** under **Private**.
    5. Select **Save changes**.

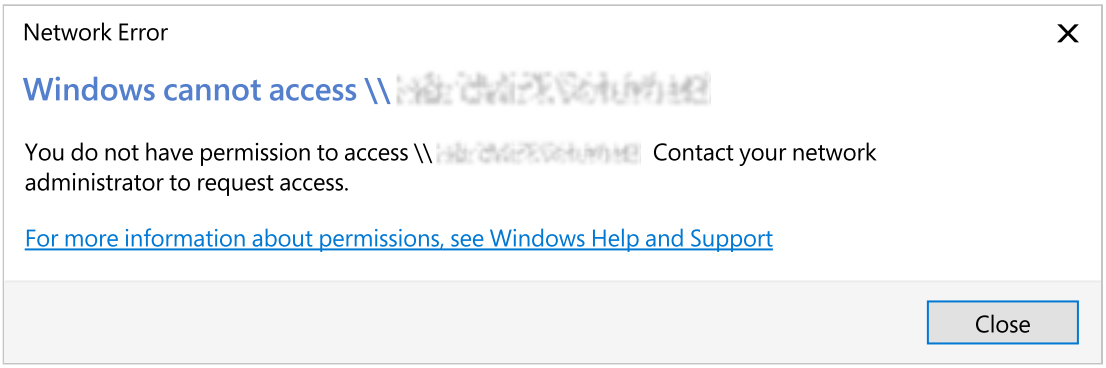


- Set the startup type of specified services to **Automatic** to make the computer visible on the network. Here's how to proceed:

    1. Go to Start.
    2. Go to Search, enter the word *Services*, and press Enter.
    3. Change the **Startup type** property to **Automatic** for the following services.
        - **Function Discovery Provider Host**
        - **Function Discovery Resource Publication**
        - **SSDP Discovery**
        - **UPnP Device Host**
    4. Restart the system.

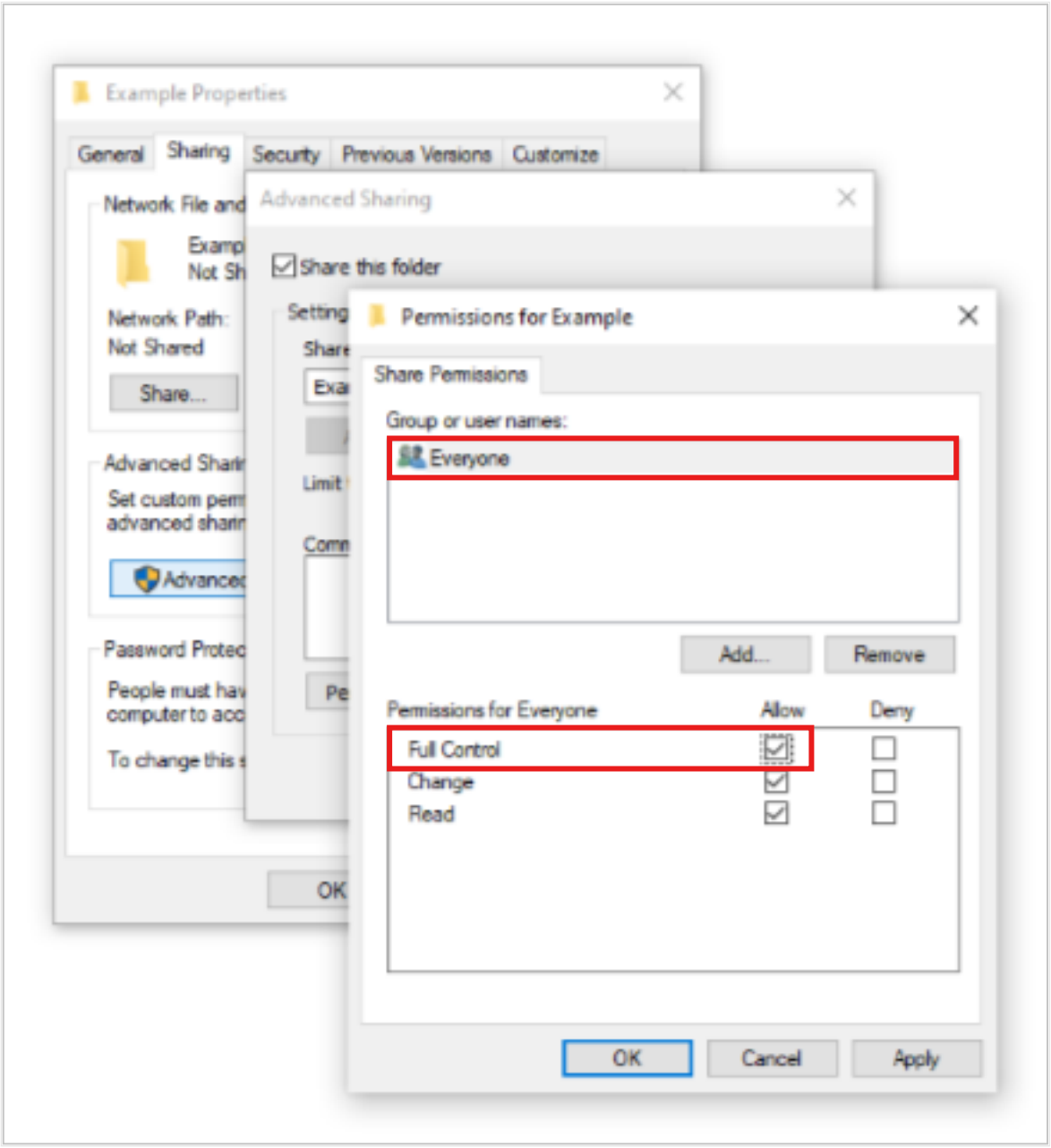
You may receive these error messages:

You do not have permission to access \\ <IPAddress or Hostname>

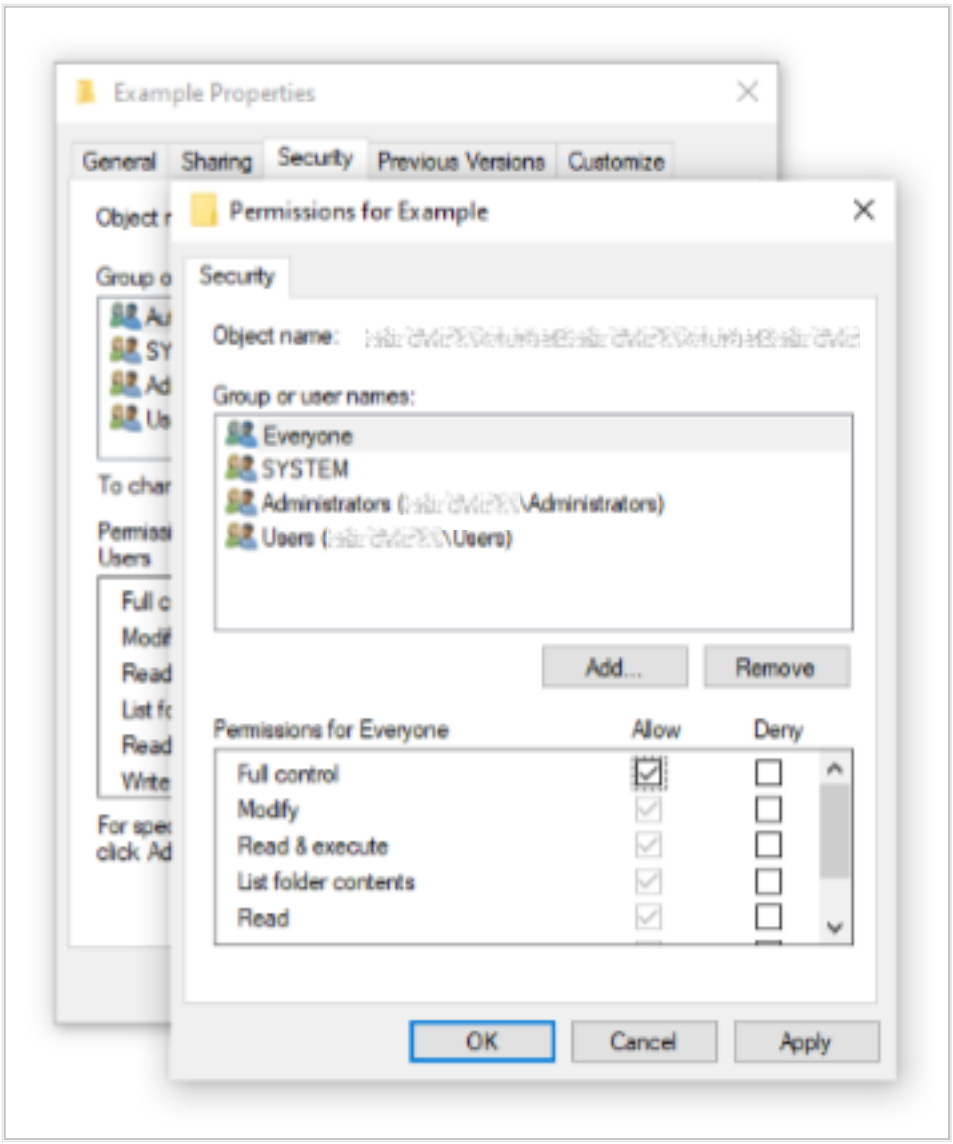


Resolution

1. Here's how to share permission to **Everyone** for the folder you want to share:
   a. Press and hold (or right-click) the shared folder.
   b. Select **Properties**, and then select **Advanced Sharing** on the **Sharing** tab.
   c. Select **Permissions**, check **Allow** for **Full Control** of **Everyone**, and then press Enter.
   d. Select **OK** on the **Advanced Sharing** dialog box.



2. Here's how to allow the **Full Control** permission to **Everyone**:
   a. Select **Edit** on the **Security** tab.
   b. Select **Add**, enter *Everyone* in the **Enter the object names to select** field, and then press Enter.
   c. Check **Allow** for **Full control** of **Everyone**, and press Enter.
   d. Close the **Properties** dialog box.

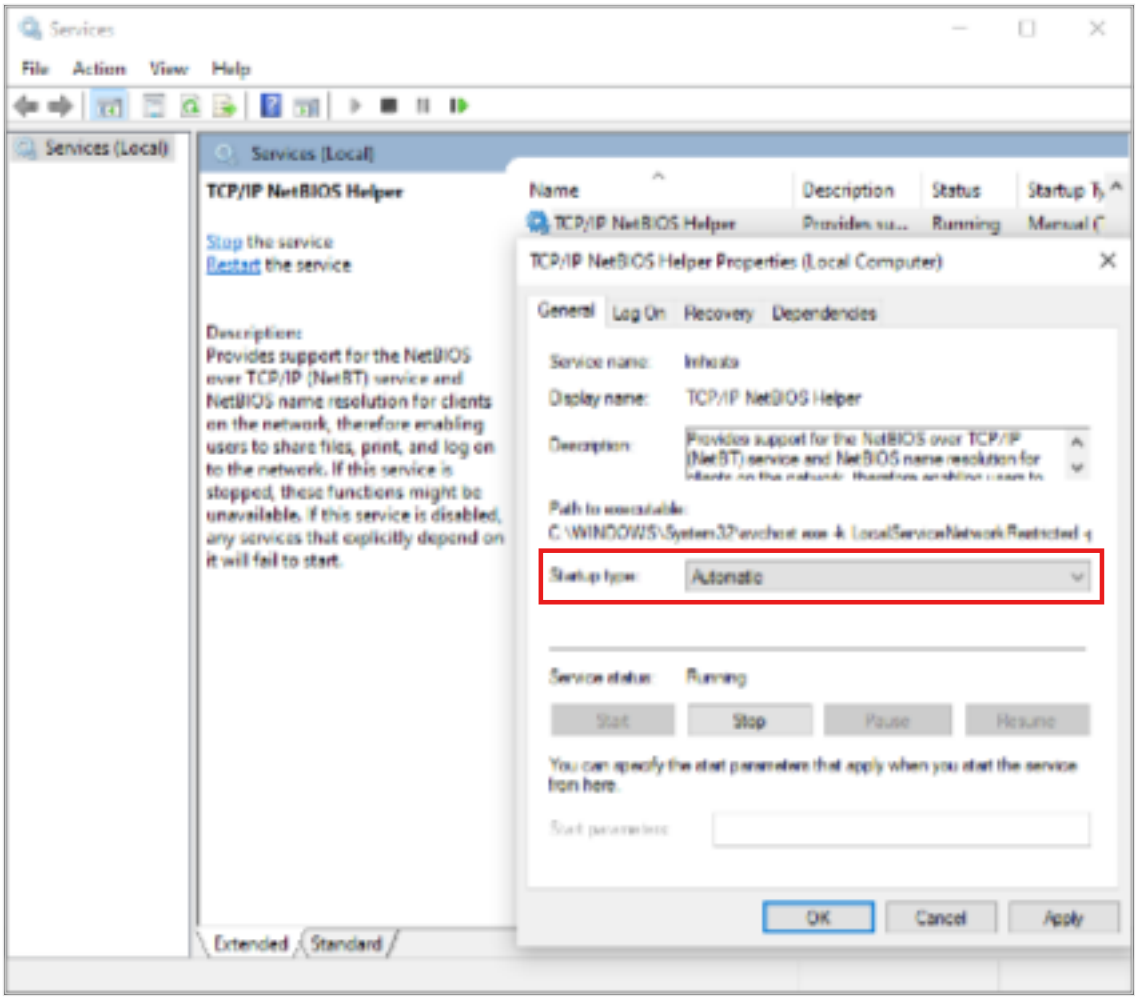


3. Here's how to make sure TCP/IP NetBIOS is enabled:

   a. Go to Start.

   b. Go to Search, enter the word *Services*, and press Enter.

   c. Double-click **TCP/IP NetBIOS Helper** on the right pane, and make sure the **Startup type** property is set to **Automatic**.

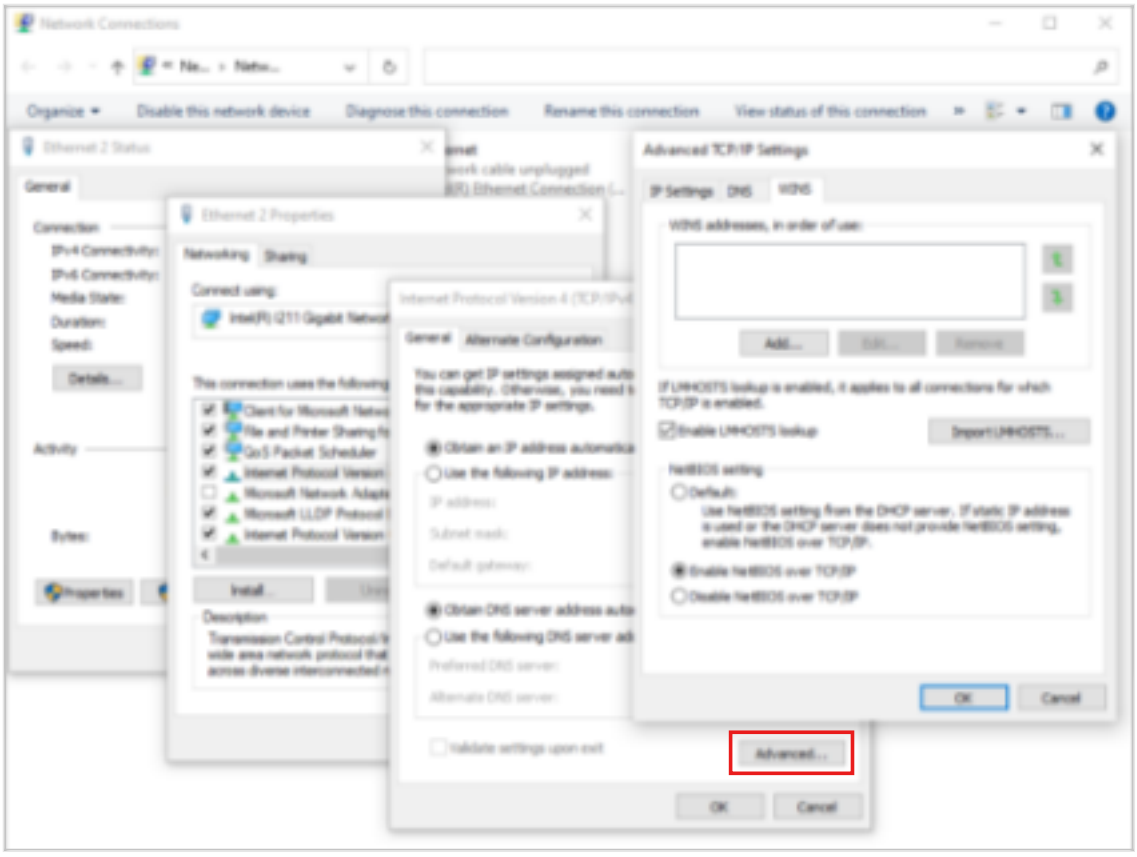


d. Go to **Control Panel** > **Network and Internet** > **Network and Sharing Center**, select **Change adapter settings** on the left pane, and then double-click **Ethernet**.

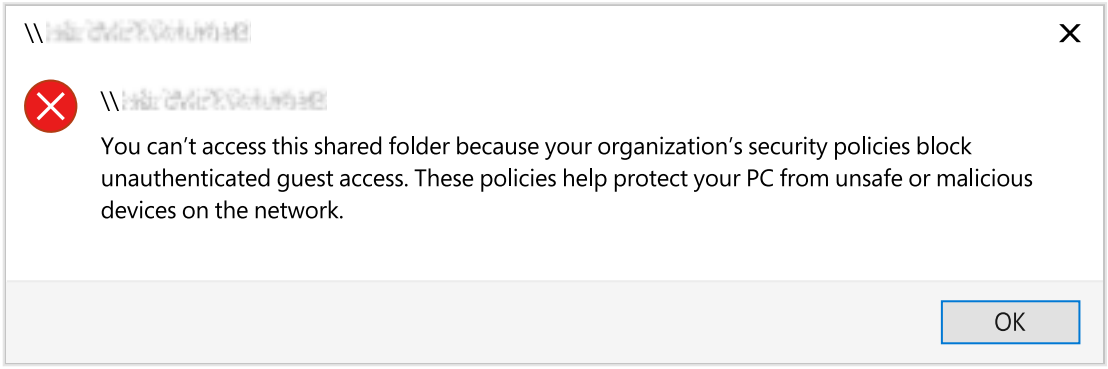
e. Select **Properties** and double-click **Internet Protocol Version 4 (TCP/IPv4)** on the **Networking** tab.

f. Select **Advanced**, select **Enable NetBIOS over TCP/IP** on the **WINS** tab, and then press Enter.

g. Select **OK** twice to close the dialog box.



You can't access this shared folder because your organization's security policies block unauthenticated guest access



Resolution

You can enable the guest access from your computer by using one of the following methods:

Method 1: Enable insecure guest logons with **Registry Editor**

1. Open **Registry Editor**.

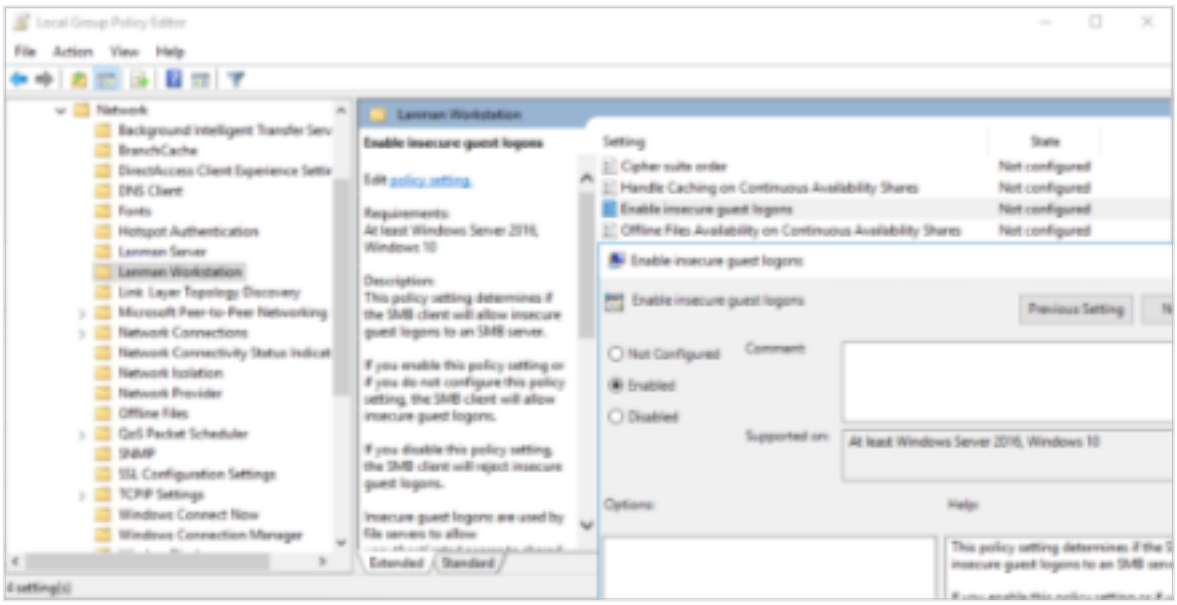
2. Go to `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation`.

> **Note**
>
> You must create the key if it doesn't exist. Press and hold (right-click) **Windows**, select **New** > **Key**, and then name the key *LanmanWorkstation*.

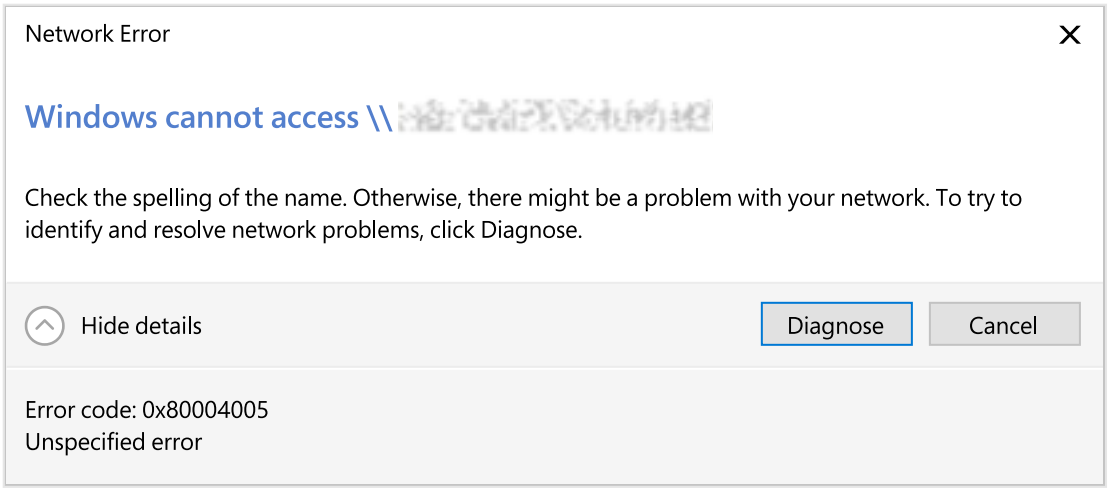
3. Press and hold (right-click) **LanmanWorkstation**, select **New** > **DWORD (32-bit) Value**, and then name it *AllowInsecureGuestAuth*. Double-click it, set the **Value data** to *1*, and then press Enter.

Method 2: Enable insecure guest logons with **Local Group Policy Editor**

1. Go to Start.
2. Go to Search, enter the word *gpedit.msc*, and then press Enter.
3. Go to **Computer Configuration** > **Administrative templates** > **Network** > **Lanman Workstation**.
4. From the right-side pane, double-click **Enable insecure guest logons**.
5. Select **Enabled**, and then press Enter.



Error code: 0x80004005. Unspecified error



Instead of obtaining an IP address automatically, specify an IP address. Follow these instructions:

1. Select **Use the following IP address** if you want to specify the IP address for the network adapter.
2. In the **IP address** box, type the IP address that you want to assign to this network adapter. This IP address must be a unique address in the range of addresses that are available for your network. Contact the network administrator to obtain a list of valid IP addresses for your network.
3. In the **Subnet mask** box, type the subnet mask for your network.
4. In the **Default gateway** box, type the IP address of the computer or device on your network that connects your network to another network or to the Internet.
5. In the **Preferred DNS server** box, type the IP address of the computer that resolves host names to IP addresses.
6. In the **Alternate DNS server** box, type the IP address of the DNS computer that you want to use if the preferred DNS server becomes unavailable.
7. Select **OK**. In the **Local Area Connection Properties** dialog box, select **Close**.
8. In the **Local Area Connection Status** dialog box, select **Close**.

Error when you try to access an administrative share on a Windows Vista-based computer from another Windows Vista-based computer that's a member of a workgroup: Logon unsuccessful: Windows is unable to log you on

Article • 09/23/2021 • 4 minutes to read

This article describes a logon unsuccessful behavior when you try to access an administrative share on a Windows Vista-based computer from another Windows Vista-based computer that's a member of a workgroup.

Applies to: Windows Vista
Original KB number: 947232

Support for Windows Vista without any service packs installed ended on April 13, 2010. To continue receiving security updates for Windows, make sure you're running Windows Vista with Service Pack 2 (SP2). For more information, see this Microsoft web page: Support is ending for some versions of Windows.

Error message description

Consider the following scenario:

- You work on a Windows Vista-based computer that's a member of a workgroup.
- From this computer, you try to access an administrative share that's located on another Windows Vista-based computer.
- The computer that you try to access is a member of a workgroup or a member of a domain. For example, you try to access the C$ administrative share.
- When you're prompted for your user credentials, you provide the user credentials of an administrative user account on the destination computer.

In this scenario, you receive the following error message:

> Logon unsuccessful:
> Windows is unable to log you on.

> Make sure that your user name and password are correct.

If you try to map a network drive to the administrative share by using the Net Use command, you receive the following error message after you provide the correct credentials:

> System error 5
> has occurred. Access is denied.

Cause

By default, Windows Vista and newer versions of Windows prevent local accounts from accessing administrative shares through the network.

Resolution

To let users have access, we recommend that you create shares on the Windows Vista-based computer by using the appropriate permissions. If, for some reason, you can't apply this resolution, you might want to try the workaround.

To share a folder on a Windows Vista-based computer that has file sharing enabled, follow these steps:

1. Click **Start** > **Computer**.
2. Locate the folder that you want to share.
3. Right-click the folder that you want to share, and then click **Share**.
4. If you have password protected sharing enabled, select which users can access the shared folder and their permission level. To let all users have access, select **Everyone** in the list of users. By default, the permission level is "Reader." Users who have this permission level can't change files or create new files in the share. To let a user change files, change folders, create new files, and create new folders, use the "Co-owner" permission level.

   If you have password protected sharing disabled, select the **Guest** account or the **Everyone** account. This is the same as simple sharing in Windows XP.
5. Click **Share** > **Done**.

Workaround

To allow administrative share access in a workgroup for Windows, use the following workaround.

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:
>
> 322756 How to back up and restore the registry in Windows

1. Click **Start**, type *regedit* in the **Start Search** box, and then press Enter.

   > **Note**
   >
   > If you're prompted for an administrator password or for confirmation, type the password or provide confirmation.

2. Locate and then click the following registry subkey:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
   ```

3. On the **Edit** menu, point to **New**, and then click **DWORD (32-bit) Value**.
4. Type LocalAccountTokenFilterPolicy to name the new entry, and then press Enter.
5. Right-click **LocalAccountTokenFilterPolicy**, and then click **Modify**.
6. In the **Value data** box, type *1*, and then click **OK**.
7. Exit Registry Editor.

The LocalAccountTokenFilterPolicy entry in the registry can have a value of 0 or 1. These values set the behavior of the entry as follows:

- 0 = build a filtered token

This is the default value. The administrator credentials are removed. These credentials are required for remote administration of the print drivers.

- 1 = build an elevated token

This value enables the remote administration of the print drivers on a server within a workgroup.

Did this fix the problem?

Check whether the problem is fixed. If it's fixed, you're finished with this article. If it isn't fixed, you can contact support.

Status

This behavior is by design.

More information

When the destination Windows Vista-based computer and the computer from which you want to access the administrative share are on the same domain, you can access the share by using domain administrator credentials.

You can't access this administrative share if the destination Windows Vista-based computer is joined to a domain and you try to connect to it by using a computer that is joined to a workgroup. This is true even if you supply correct domain administrator credentials for the domain where the destination computer is located.

For more information about how to share folders or printers in Windows Vista, visit the following Microsoft Web site:

File and Printer Sharing in Windows Vista

Mapped drive connection to network share may be lost

Article • 09/23/2021 • 3 minutes to read

This article provides solutions to an issue where the mapped drive may be disconnected if you map a drive to a network share.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 297684

Symptoms

On a computer that runs Windows 7 Service Pack 1, if you map a drive to a network share, the mapped drive may be disconnected after a regular interval of inactivity, and Windows Explorer may display a red X on the icon of the mapped drive. However, if you try to access or browse the mapped drive, it reconnects quickly.

Cause

This behavior occurs because the systems can drop idle connections after a specified time-out period (by default, 15 minutes) to prevent wasting server resources on unused sessions. The connection can be re-established quickly, if necessary.

Resolution

To resolve this behavior, change the default time-out period on the shared network computer. To do this, use one of the following methods.

Method 1: Using Registry Editor

> ⚠ **Warning**
>
> If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

Use Registry Editor to increase the default time-out period. To do this, follow these steps, and then quit Registry Editor:

> ⓘ **Note**
>
> You can't use this method to turn off the **autodisconnect** feature of the Server service. You can only use this method to change the default time-out period for the **autodisconnect** feature.

1. Click **Start**, click **Run**, type *regedit*, and then click **OK**.
2. Locate and then click the following key in the registry:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters`

3. In the right pane, click the **autodisconnect** value, and then on the **Edit** menu, click **Modify**. If the **autodisconnect** value doesn't exist, follow these steps:
   a. On the **Edit** menu, point to **New**, and then click **REG_DWORD**.
   b. Type **autodisconnect**, and then press ENTER.
4. On the **Edit** menu, click **Modify**.
5. Click **Hexadecimal**.
6. In the **Value data** box, type *ffffffff*, and then click **OK**.

The client-side session is automatically disconnected when the idling time lasts more than the duration that is set in **KeepConn**. Therefore, the session is disconnected according to the shorter set duration value between **AutoDisConnect** and **KeepConn**. To change the time-out duration in the client-side during a UNC connection, specify the arbitrary time in **KeepConn**. Locate and then click the following key in the registry:

- Location: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanworkstation\parameters`
- Value: **KeepConn**
- Data type: REG_DWORD
- Range: 1 to 65535 (sec)
- Default value: 600 sec = 10 mins

Method 2: Using Command line

> **Note**
>
> If you use this method, you may turn off the **autotuning** feature for the Server service.

To change the default time-out period for the **autodisconnect** feature of the Server service, open a command prompt, type the following line, and then press ENTER:

```
Console

net config server /autodisconnect: number
```

where *number* is the number of minutes that you want the server to wait before it disconnects a mapped network drive. The maximum value for this command is **65,535**.

> **Note**
>
> If you set the **autodisconnect** value to **0** (zero), the **autodisconnect** feature is not turned off, and the Server service disconnects mapped network drives after only a few seconds of idle time.

To turn off the **autodisconnect** feature, open a command prompt, type the following line, and then press ENTER:

```
Console

net config server /autodisconnect:-1
```

Did this fix the problem

Check whether the problem is fixed. If the problem is fixed, you are finished with this section. If the problem is not fixed, you can contact support.

More information

Some earlier programs may not save files or access data when the drive is disconnected. However, these programs function normally before the drive is disconnected.

For more information about how to increase the default time-out period, Server service configuration and tuning

Mapped drives are not available from an elevated prompt when UAC is configured to Prompt for credentials

Article • 09/23/2021 • 2 minutes to read

This article provides methods to solve the issue that mapped drives are unavailable in an elevated command prompt.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 3035277

Symptoms

This issue occurs when the following conditions are true:

- You use Group Policy Preference (GPP) or logon scripts to map network drives during logon.
- User Account Control (UAC) is enabled.
- The following UAC Group Policy setting is configured to Prompt for credentials: **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**
- The `EnableLinkedConnections` registry entry is configured. See the detail to configure the EnableLinkedConnections registry entry.

Under these conditions, you experience the following situation:

- When you sign in to the client, mapped drives are available as expected.
- When you run an elevated command prompt as administrator, the mapped drives are unavailable in the elevated command prompt.

> **Note**
>
> This issue also affects other applications that run in an elevated context (run as administrator) and use drive letters to access mapped drives.

Cause

When UAC is enabled, the system creates two logon sessions at user logon. Both logon sessions are linked to one another. One session represents the user during an elevated session, and the other session where you run under least user rights.

When drive mappings are created, the system creates symbolic link objects (DosDevices) that associate the drive letters to the UNC paths. These objects are specific for a logon session and are not shared between logon sessions.

> ⓘ **Note**
>
> The `EnableLinkedConnections` registry entry forces the symbolic links to be written to both linked logon sessions that are created, when UAC is enabled.

When the UAC policy is configured to **Prompt for credentials**, a new logon session is created in addition to the existing two linked logon sessions. Previously created symbolic links that represent the drive mappings will be unavailable in the new logon session.

Workaround - Method 1

1. In Local Group Policy Editor, locate the following Group Policy path:
   Local Computer Policy\Windows Settings\Security Settings\Local Policies\Security Options
2. Configure the following policy to **Prompt for consent**: **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**

Workaround - Method 2

Map the required drives again in the elevated session, for example, by using a .bat script file.

Detail to configure the EnableLinkedConnections registry entry

1. In Registry Editor, locate and then click the following registry subkey:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
2. Right-click **Configuration**, select **New**, and then select **DWORD (32-bit) Value**.
3. Name the new registry entry as *EnableLinkedConnections*.
4. Double-click the **EnableLinkedConnections** registry entry.

5. In the **Edit DWORD Value** dialog box, type *1* in the **Value data** field, and then select **OK**.
6. Exit Registry Editor, and then restart the computer.

Mapped network drive may fail to reconnect in Windows 10, version 1809

Article • 08/12/2022 • 3 minutes to read

This article provides a workaround for the issue that mapped network drive may fail to reconnect in Windows 10, version 1809.

Applies to: Windows 10, version 1809
Original KB number: 4471218

Symptoms

You experience the following issues in Windows 10, version 1809:

- In Windows Explorer, a red X appears on the mapped network drives.
- Mapped network drives are displayed as **Unavailable** when you run the `net use` command at a command prompt.
- In the notification area, a notification displays the following message:

> Could not reconnect all network drives.

Workaround

Microsoft is working on a resolution and estimates a solution will be available by the end of November 2018. Monitor the mapped drive topic in the Windows 10 1809 Update History KB 4464619. Currently, you can work around this issue by running scripts to automatically reconnect mapped network drive when you log on the device. To do this, create two script files, and then use one of the workarounds, as appropriate.

Create a script file named MapDrives.cmd

The file should be run at a regular but not at an elevated command prompt because it should be run at the same privilege as Windows Explorer:

PowerShell

```
PowerShell -Command "Set-ExecutionPolicy -Scope CurrentUser Unrestricted" >>
"%TEMP%\StartupLog.txt" 2>&1
PowerShell -File "%SystemDrive%\Scripts\MapDrives.ps1" >>
"%TEMP%\StartupLog.txt" 2>&1
```

Create a script file named MapDrives.ps1

The file should be run at a regular but not at an elevated command prompt because it should be run at the same privilege as Windows Explorer:

PowerShell

```
$i=3
while($True){
    $error.clear()
    $MappedDrives = Get-SmbMapping |where -property Status -Value
Unavailable -EQ | select LocalPath,RemotePath
    foreach( $MappedDrive in $MappedDrives)
    {
        try {
            New-SmbMapping -LocalPath $MappedDrive.LocalPath -RemotePath
$MappedDrive.RemotePath -Persistent $True
        } catch {
            Write-Host "There was an error mapping $MappedDrive.RemotePath
to $MappedDrive.LocalPath"
        }
    }
    $i = $i - 1
    if($error.Count -eq 0 -Or $i -eq 0) {break}

    Start-Sleep -Seconds 30
}
```

Workarounds

All workarounds should be executed in standard user security context. Executing scripts in an elevated security context will prevent mapped drives from being available in the standard user context.

Workaround 1: Create a startup item

> ⓘ **Note**
>
> This workaround works only for the device that has network access at logon. If the device has not established a network connection by the time of logon, the startup script won't automatically reconnect network drives.

1. Copy the script file (MapDrives.cmd) to the following location:
   %ProgramData%\Microsoft\Windows\Start Menu\Programs\StartUp

2. Copy the script file (MapDrives.ps1) to the following location: %SystemDrive%\Scripts\
3. A log file (StartupLog.txt) will be created in the %TEMP%\ folder.
4. Log off, and then log back on to the device to open the mapped drives.

Workaround 2: Create a scheduled task

> ⓘ **Note**
>
> A PowerShell window flashes up when the scheduled task runs.

1. Copy the script file MapDrives.ps1 to the following location: %SystemDrive%\Scripts\
2. In **Task Scheduler**, select **Action** > **Create Task**.
3. On the **General** tab in the **Create Task** dialog box, type a name (such as *Map Network Drives*) and description for the task.
4. Select **Change User or Group**, select a local user or group (such as **LocalComputer\Users**) and then select **OK**.
5. On the **Triggers** tab, select **New**, and then select **At log on** for the **Begin the task** field.
6. On the **Actions** tab, select **New**, and then select **Start a program** for the **Action** field.
7. Type *Powershell.exe* for the **Program/script** field.
8. In the **Add arguments (optional)** field, type the following: *-windowstyle hidden -command .\MapDrives.ps1 >> %TEMP%\StartupLog.txt 2>&1*
9. In the **Start in (optional)** field, type the location (*%SystemDrive%\Scripts*) of the script file.
10. On the **Conditions** tab, select the **Start only if the following network connection is available** option, select **Any connection**, and then select **OK**.
11. Log off, and then log back on to the device to run the scheduled task.

Saving and restoring existing Windows shares

Article • 09/23/2021 • 3 minutes to read

This article provides some information about saving and restoring existing Windows shares.

Applies to: Windows Server 2012 R2
Original KB number: 125996

Summary

If you need to complete any of the following procedures, you can save the share names that exist on the original Microsoft Windows installation, including any permissions assigned to those shares:

- Reinstall Windows over an existing installation (a clean install, not an upgrade).
- Move all of your data drives from one server to another.
- Install Windows to another folder or drive on a computer that already has Windows installed.

More information

For information on how administrators can migrate data safely and reliably from one file server to another file server, visit the following Microsoft Web site:
Microsoft File Server Migration Toolkit .

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base: **322756** How to back up and restore the registry in Windows.

To save only the existing share names and their permissions on Windows follow these steps.

> ⓘ **Note**
>
> This procedure applies only to NetBIOS shares and not to Macintosh volumes.

1. On the existing Windows installation that contains the share names and permissions that you want to save, start **Registry Editor** (Regedt32.exe).
2. From the HKEY_LOCAL_MACHINE subtree, go to the following key: `SYSTEM\CurrentControlSet\Services\LanmanServer\Shares`.
3. Save or export the registry key.
   - For Windows NT and Windows 2000, click **Save Key** on the Registry menu.
   - For Windows Server 2003, click **Export** on the **File** menu.
4. Type a new file name (a file extension is not necessary), and then save the file to a floppy disk.
5. Reinstall Windows.
6. Run **Registry Editor** (Regedt32.exe).
7. From the HKEY_LOCAL_MACHINE subtree, go to the following key: `SYSTEM\CurrentControlSet\Services\LanmanServer\Shares`.
8. Restore or import the registry key.
   - For Windows NT and Windows 2000, click **Restore** on the Registry menu.
   - For Windows Server 2003, click **Import** on the **File** menu.
9. Type the path and file name of the file that you saved in steps 3 and 4.

   > ⊗ **Caution**
   >
   > This step overrides the shares that already exist on the Windows computer with the share names and permissions that exist in the file you are restoring. You are warned about this before you restore the key.

10. Restart the server.

> ⓘ **Note**

After you complete this procedure, if you decide that you should not have restored the Shares key, restart the computer and press the SPACEBAR to use the last known good configuration. After you restore the shares key, the shares can be used by network clients. If you run the net shares command on the server, the server displays the shares; however, File Manager does not display the shares. To make File Manager aware of the newly restored shares, create any new share on the server. File Manager displays all of the other shares after you restart the server or stop and restart the Server service.

In Windows NT 3.5, if you click Stop Sharing in File Manager, the restored shares are still displayed, but they are dimmed.

Only permissions for domain users are restored. If a local user was created in the previous Windows NT installation, that local user's unique security identifier (SID) is lost. NTFS permissions on folders and files are not affected when you save and restore the shares key.

Slow network performance when you open a file that is located in a shared folder on a remote network computer

Article • 09/23/2021 • 3 minutes to read

This article helps fix a slow network performance issue that can occur when you open a file that is located in a shared folder on a remote network computer.

Applies to: Windows 7 Service Pack 1
Original KB number: 829700

Symptoms

When you use Windows Explorer to connect to a shared folder on a remote computer on your network, and you double-click a file in that shared folder to open it, it may take a longer time than expected to open the file. For example, you may experience this issue when you open a Microsoft Office document over a slow connection, such as a 64-kilobits-per-second (kbps) Integrated Services Digital Network (ISDN) connection on a wide area network (WAN).

Cause

This issue occurs because Windows Explorer tries to obtain detailed information about the remote share and about the file that you are opening. This operation may take a long time over a slow connection.

Resolution

Important

This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base: 322756 How to back up and restore the registry in Windows

1. Add the **SuppressionPolicy** DWORD value to the following registry key:
   `HKEY_CLASSES_ROOT\*\Shellex\PropertySheetHandlers\CryptoSignMenu`
   To do so:
   a. Click **Start**, and then click **Run**.
   b. In the **Open** box, type regedit, and then click **OK**.
   c. Locate and then click the following registry key:
   `HKEY_CLASSES_ROOT\*\Shellex\PropertySheetHandlers\CryptoSignMenu`
   d. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
   e. Type SuppressionPolicy, and then press ENTER.
   f. On the **Edit** menu, click **Modify**.
   g. Click **Hexadecimal**, type 100000 in the **Value data** box, and then click **OK**.
2. Add the **SuppressionPolicy** DWORD value to the following registry key:
   HKEY_CLASSES_ROOT*\Shellex\PropertySheetHandlers\{3EA48300-8CF6-101B-84FB-666CCB9BCD32}
   To do so:
   a. In Registry Editor, locate and then click the following registry key:
   HKEY_CLASSES_ROOT*\Shellex\PropertySheetHandlers\{3EA48300-8CF6-101B-84FB-666CCB9BCD32}
   b. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
   c. Type SuppressionPolicy, and then press ENTER.
   d. On the **Edit** menu, click **Modify**.
   e. Click **Hexadecimal**, type 100000 in the **Value data** box, and then click **OK**.
3. Add the **SuppressionPolicy** DWORD value to the following registry key:
   HKEY_CLASSES_ROOT*\Shellex\PropertySheetHandlers\{883373C3-BF89-11D1-BE35-080036B11A03}
   To do so:
   a. In Registry Editor, locate and then click the following registry key:
   HKEY_CLASSES_ROOT*\Shellex\PropertySheetHandlers\{883373C3-BF89-11D1-BE35-080036B11A03}
   b. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
   c. Type SuppressionPolicy, and then press ENTER.

d. On the **Edit** menu, click **Modify**.
e. Click **Hexadecimal**, type 100000 in the **Value data** box, and then click **OK**.

4. Add the **Flags** DWORD value to the following registry key:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SCAPI`
   To do so:

   a. In Registry Editor, locate and then click the following registry key:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SCAPI`

   b. On the **Edit** menu, point to **New**, and then click **DWORD Value**.

   c. Type Flags, and then press ENTER.

   d. On the **Edit** menu, click **Modify**.

   e. Click **Hexadecimal**, type 00100c02 in the **Value data** box, and then click **OK**.

   f. Quit Registry Editor.

Adding a Group Policy

Besides the direct registry modifications that are described in the "Changing the registry" section, you can also resolve this issue by using a Group Policy. Administrators can control which shell extensions can run by using the **Approved** key and the EnforceShellExtensionSecurity policy. The SuppressionPolicy value is tied to the EnforceShellExtensionSecurity policy. You can add this policy to enable the modified shell behavior.

To do this, follow these steps:

1. Click **Start**, click **Run**, type Gpedit.msc, and then click **OK**.
2. Under **User Configuration** in the left pane, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Explorer**.
3. In the right pane, double-click **Allow only per user or approved shell extensions**, click **Enabled**, and then click **OK**.

System error 85 with the NET USE command

Article • 09/23/2021 • 2 minutes to read

This article helps fix the system error 85 that occurs when a non-administrative user attempts to reconnect to a shared network drive that the user has already used by using the `net use` command.

Applies to: Windows 10 - all editions
Original KB number: 253821

Symptoms

When a non-administrative user attempts to reconnect to a shared network drive that the user has already used, system error 85 (Local device name already in use) may be generated.

For example, running the following sequence of commands in a logon script or from a command prompt illustrates the issue:

Console

```
net use r: /d
net use r: \\servername\share
net use r: /d
net use r: \\servername\share
```

The behavior does not occur for users with administrative privileges.

Cause

This behavior is caused by a setting of **1** in the following registry value:
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\ProtectionMode`

If the setting is **1**, the problem occurs. If you change the setting to **0** and reboot the server, the problem disappears.

Note

We suggest changing this value to 1 to restrict changes to Base System objects and for solving problems with symbolic links.

Workaround

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

Change the entry for `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\ProtectionMode` from **1** to **0**.

> **Note**
>
> If you are running a Windows Server 2003-based Terminal Server, set the `ProtectionMode` to a value of **1**. Error 85 translates to the following: ERROR_ALREADY_ASSIGNED The local device name is already in use.

How to configure a domain suffix search list on the Domain Name System clients

Article • 09/23/2021 • 2 minutes to read

This article describes how to automate the process of configuring the domain suffix search list on your Domain Name System (DNS) clients.

> **Note**
>
> This article applies to Windows 2000. Support for Windows 2000 ends on July 13, 2010. The Windows 2000 End-of-Support Solution Center is a starting point for planning your migration strategy from Windows 2000. For more information, see the **Microsoft Support Lifecycle Policy**.

Applies to: Windows Server 2012 R2
Original KB number: 275553

Summary

This article does not describe when it is necessary to configure the domain suffix search list on a client. This article only describes how to distribute a large-scale domain suffix search list.

More Information

The typical name resolution process for Microsoft Windows 2000 uses the primary DNS suffix and any connection-specific DNS suffixes. If these suffixes do not work, the devolution of the primary DNS suffix is attempted by the name resolution process.

When a domain suffix search list is configured on a client, only that list is used. The primary DNS suffix and any connection-specific DNS suffixes are not used, nor is the devolution of the primary suffix attempted. The domain suffix search list is an administrative override of all standard Domain Name Resolver (DNR) look-up mechanisms.

For more information about how DNS suffixes are used, go to Windows 2000 Help and view the Configuring Client Settings topic (located in the Networking/DNS/Concepts/Using DNS/Managing Clients/ folder).

Pushing the domain suffix search list to DNS clients

The following methods of distribution are available for pushing the domain suffix search list to DNS clients:

- Regini.exe. The Regini.exe tool from the Microsoft Windows 2000 Resource Kit can be used to place the domain suffix search list setting into the registry. A sample Regini script is provided in the "Sample Regini Script" section of this article.
- Unattended installation. You can populate the domain suffix search list settings during an unattended installation.

The following methods of distribution are not available for pushing the domain suffix search list to DNS clients:

- Dynamic Host Configuration Protocol (DHCP). You cannot configure DHCP to send out a domain suffix search list. This is currently not supported by the Microsoft DHCP server.
- Netsh (Netshell). The Netsh utility has no command to set or to change the domain suffix search list.
- Group Policy. In Windows 2000, Group Policy has no mechanism for distributing the domain suffix search list. However, Windows Server 2003 includes this feature.
- Microsoft Visual Basic Scripting Edition (VBScript). No application programming interfaces (APIs) are available that enable you to script a change to the domain suffix search list.

Sample Regini script

Create a text file with the following two lines of text and save it as the Suffix.txt file. The following spacing must be exactly as shown, where `adatum.xxx` signifies a domain suffix. Up to six domain suffixes may be specified. The search order is left to right.

```
\Registry\Machine\System\CurrentControlSet\Services\TCPIP\Parameters
SearchList="testadatum.com,test2adatum.net,test3adatum.gov"
```

Copy the Regini.exe and Suffix.txt files to the preceding location and run the regini.exe suffix.txt command.

When the script has updated the registry, you must restart the computer for the settings to be updated.

To run the script, you must have administrator or system-level access to the computer.

> ⓘ **Note**

Another method is to use Microsoft Windows Script Host:

1. Create a file with the .vbs extension (for example, C:\add.vbs).

2. Add the following two lines to the file:

   Visual Basic Script

   ```
   SET WSHShell = CreateObject("WScript.Shell")
   WSHShell.RegWrite
   "HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\SearchList
   ", "testadatum.com,test2adatum.net,test3adatum.gov", "REG_SZ"
   ```

   (the second line starts with "WSHShell.RegWrite" and ends with "REG_SZ")

3. Double-click the file to run or at a command prompt, type *C:\add.vbs*

DNS requests appear to be random after startup or network properties change

Article • 09/23/2021 • 2 minutes to read

This article provides some information about DNS requests that appear to be random after startup or network properties change.

Applies to: Windows 10 - all editions
Original KB number: 4564934

Summary

You have a computer that runs Windows 8 or a later version, and has at least one network adapter that is configured as follows:

- The adapter is not connected to a domain network
- The adapter does not have a WINS server configured

After the computer starts or after a network property changes, you may observe that the computer sends out one or two DNS name resolution requests that appear to be random.

Cause

In certain circumstances, the Windows DNS client may send DNS name resolution requests that appear to be random. These requests serve various purposes, such as detecting network conditions. This Windows request behavior is subject to change.

More information

When the queries are sent by the Windows DNS client, no action is required. Blocking these queries may affect Windows performance.

URI-encoding in UNC paths interpreted literally in Windows 10, version 1803 and later

Article • 09/23/2021 • 2 minutes to read

This article provides some information about URI-encoding in UNC paths interpreted literally in Windows 10, version 1803 and later.

Applies to: Windows 10 - all editions
Original KB number: 4467268

Summary

In Windows 10, version 1803 and later versions of Windows, URLs (such as SharePoint document libraries) can't be referenced by Universal Naming Convention (UNC) paths that contain URI encoding characters.

For example, when the path `http://myserver/Shared Documents` is URI-encoded, the path becomes `http://myserver/Shared%20Documents`. Before Windows 10, version 1803, the UNC path \\myserver\shared%20documents could be used. After you upgrade to version 1803, the "%20" is no longer interpreted as a space but as the literal value "%20". This can prevent previously generated links from resolving to the correct http path.

More information

This is by design. The UNC pathing should be updated to reflect the literal path, and any URI-encoding characters should be removed. Or, use a scheme of file:// so that the path is decoded. (For example: file://\\myserver\shared%20documents.)

To achieve parity with the local Windows file system naming convention, Windows 10, version 1803 introduces support for additional characters in file names and folders on web-based paths.

One of the previously unsupported characters is the percent sign (%). Because this character is the escape character that's used for URI encoding, a UNC path that has been URI-encoded will no longer be URI decoded. Instead, it will be treated as a literal path.

Windows style paths are not URIs and thus don't follow normal URI-encoding rules, so any characters that use percent encoding in URIs should be decoded when translating WebDAV-style paths back into Windows-style paths. Similarly, Windows-style paths don't use percent-encoding to represent special characters in file names, so whenever the WebClient service observes a percent character in a Windows style path when translating to a URI, the "%" character will be replaced by "%25" even when the "%" character is followed by two hex digits.

Support policy for DNS client-side caching on DNS clients

Article • 12/15/2021 • 2 minutes to read

Windows contains a client-side DNS cache. Microsoft doesn't recommend disabling DNS client-side caching on DNS clients. A configuration in which DNS client-side caching is disabled isn't supported.

Support policy

Microsoft does not guarantee that a resolution will be found for issues that involve unsupported devices or configuration. If no resolution is found, the cost of an investigation into the incident is not refunded. If it is not agreed that a solution is not guaranteed, Microsoft Support will not fix the problem and will refund the cost of investigating the incident.

DHCP clients are blocked when a DAI-enabled network device is used with a DHCP failover in Windows Server 2012 R2

Article • 09/23/2021 • 3 minutes to read

This article provides a workaround for an issue where DHCP clients are blocked when a DAI-enabled network device is used together with a DHCP failover on a Windows Server 2012 server.

Applies to: Windows Server 2012 R2
Original KB number: 2978225

Symptoms

Consider the following scenario:

- You deploy a Dynamic Host Configuration Protocol (DHCP) failover by using a server that is running Windows Server 2012 R2.
- In this environment, you deploy a pair of active-active (duplicate) DHCP relay agents.
- DHCP snooping and Dynamic ARP Inspection (DAI) are enabled on network devices, such as switches.

In this scenario, DHCP clients are blocked and experience other network issues.

Cause

This problem occurs because the duplicated DHCP relay agents cause the DHCP server to always receive duplicate DHCP messages for each client that connects to the network. For both DHCP requests, the DHCP failover-enabled server sends to the clients different ACK messages that have different lease duration values. This leads to a race condition in which the clients accept the first value that is received and ignore the second. However, DAI honors the second value. This creates a lease mismatch and causes DAI to block clients from accessing the network.

Workaround

To work around this problem, use one of the following methods:

- Prevent duplicate DHCP requests. To do this, use one of the following options:
  - Remove the second DHCP relay agent.
  - Operate the DHCP relay agents in an active-passive mode. To do this, use virtual router groups if your router redundancy protocol is HSRP.
- Configure DAI so that it honors the first DHCP lease duration value (whenever possible).
- If DAI can't be configured to honor the first lease duration value, turn off or remove the DAI feature that is causing the conflict.
- Don't use DHCP failover in combination with two relay agents and DAI on the switches.

More information

To provide redundancy, some organizations prefer to configure dual relays (two routers that each point to two DHCP servers). This configuration is common when Virtual Router Redundancy Protocol (VRRP) is used.

In a typical VRRP configuration that uses one IP address, one router is designated as the "active" device and the other one is set to "standby" mode. A heartbeat is exchanged between the routers. If the active router doesn't respond, the standby router takes over the shared IP address.

DHCP snooping enables a switch device to inspect DHCP traffic and to track which IP addresses are assigned to which host switch ports. This information can be useful to DAI. As soon as the DHCP lease duration expires, the traffic information is removed from the device database. A DAI-enabled switch will then block the ports.

A DHCP failover on a Windows Server 2012 server can't guarantee consistent lease duration for duplicated DHCP requests. This behavior is by design. This is because a DHCP server may issue either a Maximum Client Lead Time (MCLT) or Scope lease duration value, depending on the following circumstances:

- Upon receiving the first request, the DHCP server sends an ACK that includes an MCLT lease duration value before it tries to synchronize with its partner. This is also known as a Lazy Update.
- If the sync response arrives before the duplicated request, the DHCP server considers its partner to be up-to-date. It then sends an ACK that includes the Scope lease duration value. This is the desired behavior.

- If the duplicate request arrives before the sync response, the race condition that is described in the Cause section occurs. In this case, the DHCP server considers its partner to be out-of-sync. This causes the second ACK to use the MCLT lease duration value. You can't prevent the duplicate DHCP ACK messages from being sent. This is because a DHCP failover on a Windows Server 2012 server always responds by sending one DHCP ACK per DHCP request even though DHCP requests have the same transaction ID. This behavior is by design.

Additional information

- The DHCP transaction ID is a way for the client to relate a sent message with a received message. The RFC does not imply that the server should be dropping messages based on transaction ID.
- At this time, we believe that a design change isn't warranted, based upon the following definition of a transaction ID that is provided in RFC 2131:

> xid 4
> Transaction ID, a random number chosen by the client, used by the client and server to associate messages and responses between a client and a server.

Can't open files offline when you use Offline Files and Windows Information Protection

Article • 09/23/2021 • 2 minutes to read

This article provides workarounds for an issue that prevents you from opening files offline when you're using the Offline Files feature together with Windows Information Protection.

Applies to: Windows 10 - all editions
Original KB number: 3187045

Symptoms

Consider the following scenario:

- You have Windows 10 installed.
- Special folders (for example, Documents or Favorites) are redirected to a file share.
- User data in the redirected folders is cached locally through the Offline Files feature.
- Windows Information Protection (also known as Enterprise Data Protection) is enabled on the system.
- You're using an application that's managed by Windows Information Protection.

If you try to open a file while working offline in this scenario, the attempt fails. The error message that's displayed in this situation varies, depending on the application. Word and Excel fail with the following error:

> Sorry, we couldn't open '\\severname\fileshare\filename'

Cause

This issue occurs because the Offline Files feature doesn't support Windows Information Protection.

Workaround

To work around this issue, use one of the following methods:

- Open the file by using an application that's not managed by Windows Information Protection.
- Open the file while you're working online (connected to your corporate network).

More information

There are no plans to update Offline Files to support Windows Information Protection. We recommend that you migrate to a modern file sync solution such as Work Folders or OneDrive for Business.

For information about how to migrate from Offline Files to Work Folders see the following TechNet site:

Offline Files (CSC) to Work Folders Migration Guide

Redirecting the user's Documents folder to their home directory fails when Grant the user exclusive rights to Documents is selected

Article • 09/23/2021 • 2 minutes to read

This article helps fix an issue where you can't redirect the user's Documents folder to their home directory when "Grant the user exclusive rights to Documents" is selected.

Applies to: Windows 7 Service Pack 1
Original KB number: 2493506

Symptoms

Using Folder Redirection policy to redirect the user's Documents folder to their home directory, when "Grant the user exclusive rights to Documents" is selected, fails to create the Synchronization Partnership and fails to copy the Documents data to the home directory.

The following error is logged in the Application Event Log:

> Log Name: Application
> Source: Microsoft-Windows-Folder Redirection
> Date: <DateTime>
> Event ID: 502
> Task Category: None
> Level: Error
> Keywords:
> User: `contoso.com\jim`
> Computer: `Win7-1.contoso.com`
> Description:
> Failed to apply policy and redirect folder "Documents" to "\\`contoso.com`\home\jim\".
> Redirection options=0x1211.
> The following error occurred: "Can not create folder "\\`contoso.com`\home\jim".
> Error details: "This security ID may not be assigned as the owner of this object."

Cause

1. You have a computer running Vista SP1 or Windows 7
2. Folder Redirection Policy is configured to redirect the Documents folder to the user's home directory
3. "Grant the user exclusive rights to Documents" - enabled
4. "Also apply redirection policy to Windows 2000, Windows 200 Server, Windows XP, and Windows Server 2003 operating systems" - disabled

In this configuration, the Synchronization Partnership isn't created and therefore the documents in the home directory and local profile aren't merged.

Resolution

Do one of the following:

1. Enable both "Grant the user exclusive rights to Documents" and "Also apply redirection policy to Windows 2000, Windows 200 Server, Windows XP, and Windows Server 2003 operating systems". When both are enabled, then the Synchronization Partnership is successfully created and documents are synchronized between the local profile and the home directory.

   -- OR --

2. Disable both "Grant the user exclusive rights to Documents" and "Also apply redirection policy to Windows 2000, Windows 200 Server, Windows XP, and Windows Server 2003 operating systems". When both are disabled, then the Synchronization Partnership is successfully created and documents are synchronized between the local profile and the home directory.

How to change the location of the CSC folder by configuring the CacheLocation registry value in Windows

Article • 09/23/2021 • 2 minutes to read

This article describes how to change the location of the client-side caching (CSC) folder by configuring the CacheLocation registry value.

Applies to: Windows 10 - all editions
Original KB number: 937475

Introduction

You cannot use the Cachemov.exe tool to move the client-side caching (CSC) folder in Windows Vista. However, you can change the location of the CSC folder by configuring the CacheLocation registry value.

> **Note**
>
> The CSC folder is the folder in which Windows stores offline files.

More information

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base: 322756 How to back up and restore the registry in Windows

To change the location of the CSC folder, follow these steps.

> **Note**

There is only one cache folder in Windows Vista. Therefore, you do not have to repeat these steps for additional users.

1. Click **Start**, type **regedit** in the **Search** box, and then press ENTER.
2. Locate the following registry subkey, and then and right-click it:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CSC`
3. Point to **New**, and then click **Key**.
4. Type Parameters in the name box for the new key.
5. Right-click the **Parameters** key, point to **New**, and then click **String Value**.
6. To name the new value, type CacheLocation, and then press ENTER.
7. Right-click **CacheLocation**, and then click **Modify**.
8. In the **Value data** box, type the name of the new folder in which you want to create the cache.

   > ⓘ **Note**
   >
   > Use the Microsoft Windows NT format for the folder name.

   For example, if you want the cache location to be d:\csc, type the following: ??\d:\csc
9. Exit Registry Editor, and then restart the computer.

> ⓘ **Note**
>
> The network administrator can set this value before the computer is on the network or before this value is given to the end-user. In this situation, no content is put in the default location. Additionally, you can set the location of the CSC folder by using a script.

The information and the solution in this document represent the current view of Microsoft Corporation on these issues as of the date of publication. This solution is available through Microsoft or through a third-party provider. Microsoft does not specifically recommend any third-party provider or third-party solution that this article might describe. There might also be other third-party providers or third-party solutions that this article does not describe. Because Microsoft must respond to changing market

conditions, this information should not be interpreted to be a commitment by Microsoft. Microsoft cannot guarantee or endorse the accuracy of any information or of any solution that is presented by Microsoft or by any mentioned third-party provider.

Microsoft makes no warranties and excludes all representations, warranties, and conditions whether express, implied, or statutory. These include but are not limited to representations, warranties, or conditions of title, non-infringement, satisfactory condition, merchantability, and fitness for a particular purpose, with regard to any service, solution, product, or any other materials or information. In no event will Microsoft be liable for any third-party solution that this article mentions.
For more information about how to move the offline files cache in Windows Vista, visit the following Web site: Storage at Microsoft

Features and functions in version 1.1 of the Client-Side Caching Command-Line Options command-line tool

Article • 02/28/2022 • 8 minutes to read

This article provides information about the features and functions that are available in the offline file management tool CSCCMD 1.1.

Applies to: Microsoft Windows XP, and Microsoft Windows Server 2003. *Original KB number:* 884739

Introduction

This article contains information about the features and functions in the latest version of the Client-Side Caching Command-Line Options (CSCCMD) command-line tool (Csccmd.exe).

More information

You can use the CSCCMD tool to manage offline files in Microsoft Windows 2000, in Microsoft Windows XP, and in Microsoft Windows Server 2003. The latest version of the CSCCMD tool is 1.1. Version 1.1 includes new functions and features that weren't available in the earlier versions.

> **Note**
>
> Users who use the CSCCMD tool must have good knowledge of client-side caching functionality.

To obtain the CSCCMD tool, contact Microsoft Product Support Services. For a complete list of Microsoft Product Support Services phone numbers and information about support costs, visit the following Microsoft Web site:

Global Customer Service phone numbers

> **Note**

You can also download CSCCMD 1.0 and other tools as part of Windows Server 2003 Resource Kit Tools.

The CSCCMD tool uses the following syntax: CSCCMD [/RESID] [/ENABLE] [/DISABLE] [/DISCONNECT: **Server****Share**] [/MOVESHARE: **Server****Share1** **Server****Share2**] [/?]

The following command-line switches and their functions are available in the latest version of the CSCCMD tool:

- /ENABLE - Use this switch to enable Client-Side Caching (CSC) on a client. This switch lets you access and synchronize network files while you're working offline.

  > ⓘ **Note**
  >
  > You must be an administrator on the local computer to use this switch.

- /DISABLE - Use this switch to disable CSC. Before you run this command, you must make sure that you've closed all offline files. If you disable CSC, you can't work on network files while you're working offline.

  > ⓘ **Note**
  >
  > You must be an administrator on the local computer to use this switch.

- /ENUM[:\\ **Server****Share**[**Path**]] [/RECURSE] - Use this switch to display all the shares in the local cache. If you use this switch with the /RECURSE option, the CSCCMD tool displays the contents of the shares within a parent share. You can also display the contents of a specific share of a server. To do this, use the **Server****Share** format. For example, use the following command: CSCCMD /ENUM: **MyServer****MyShare**

  > ⓘ **Note**
  >
  > **MyServer** is the server name, and **MyShare** is the name of the shared resource.

- /DISCONNECT: **Server****Share** - Use this switch to disconnect a specific server from Client-Side Caching on the client computer. Use the **Server****Share** format to specify the name of a specific shared resource of a server that you want to disconnect. For example, use the following command: CSCCMD /DISCONNECT:

\\MyServer\MyShare
The background Client-Side Caching agent doesn't try to reconnect the server. If you synchronize offline content by using the synchronization manager, the Client-Side Caching agent then reconnects to the server if it's available.

> ⓘ **Note**
>
> A handle must be open on this share or any directory/file on this share for this function to work correctly.

- /MOVESHARE: **Server1\Share\\Server2\Share** - Use this switch to move files and directories from one share to another share in the cache. This option is useful if the target of offline files has moved and if the local cache now must point to a new location. For example, use the following command: CSCCMD /MOVESHARE: **\\MyServer\MyShare\\MyServer1\MyShare1**

  > ⓘ **Note**
  >
  > **MyServer1** is the new server name, and **MyShare1** is the name of the new shared resource.

- /RESID - Use this switch to restamp all the entries in the Windows offline files (CSC) database by using a new user security identifier (SID). This switch is used in scenarios where an organization moves user accounts from a Microsoft Windows NT 4.0 domain to a Windows Server 2003 domain.

  If a user's cache is security enhanced by using the user's Windows NT 4.0 SID, the cache can't be accessed from the Windows Server 2003 account unless the cache entries are restamped by using the Windows Server 2003 SID.

- /ISENABLED or /ISCSCENABLED - Use either of these switches to determine whether CSC is enabled on your client computer.

- /PIN2: **server\share\path**[/USER] [/SYSTEM] [/USERINHERIT] [/SYSTEMINHERIT] - Use this switch to pin shared resources. You can use the /USER option to pin a file. This action has the same result as using the **Offline Files** dialog box to cache the file. The /SYSTEM option specifies that the shared resource must be administratively pinned by configuring the Group Policy settings. The /USERINHERIT option and the /SYSTEMINHERIT]INHERIT option designates how the pin data is inherited. You can use any combination of the pin types.

- /PIN2: **filename** /FILELIST [/UNICODE] [/USER] [/SYSTEM] [/USERINHERIT] [/SYSTEMINHERIT]
- Use this switch if you want to use a file that describes all the objects to pin as parameters. The file contains the Universal Naming Convention (UNC) path of the objects to pin. The objects are separated by a carriage return/linefeed. For example, use the following command: CSCCMD /PIN: **MyShare.txt** /FILELIST

  > ⓘ **Note**
  >
  > The **MyShare.txt** file contains entries that are separated by spaces.

  These entries are similar to the following:

  //MyServer/MyShare //MyServer1/MyShare1

  > ⓘ **Note**
  >
  > The /PIN switch does not copy the content of the shared resource into the local cache. Pinning is not sufficient to make the files available offline. After you use the /PIN switch, you must run the CSCCMD command together with the /FILL switch to copy the content of the shared resource to the local cache and to make sure that the shared resource is available offline. The /USERINHERIT option and the /SYSTEMINHERIT]INHERIT option designates how the pin data is inherited. You can use any combination of the pin types.

- /UNPIN2: **server\share\path**[/USER] [/SYSTEM] [/USERINHERIT] [/SYSTEMINHERIT] [/RECURSE]
- Use this switch to unpin a shared resource or to remove a shared resource from the local cache. If you use this switch with the /RECURSE option, the CSCCMD tool unpins all children of the path. If you use this switch with the /RECURSE2 option, the CSCCMD tool unpins the path and children of the path. You can use any combination of the pin types.
- /UNPIN2: **filename** /FILELIST [/UNICODE] [/USER] [/SYSTEM] [/USERINHERIT] [/SYSTEMINHERIT] - Use this switch to unpin a specific set of shared resources by using a file. You can use any combination of the pin types.

  > ⓘ **Note**

> The /FILELIST parameter indicates that the file specified is a text file with one file name for each line. Any white space at the start of a file is ignored. However, any white space at the end of the line is counted. Lines are delimited by any combination of carriage return characters, linefeed characters, or both.

If you use this switch with the /UNICODE option, the CSCCMD tool creates the file list in Unicode text format.

- /FILL: **Server****Share****Path** - Use this switch to copy server-side data to the local cache for a specified shared resource.
- /FILL: **FileName** /FILELIST [/UNICODE]
- Use this switch to copy server-side data to the local cache for a set of specified shared resources by using a file.

  > ⓘ **Note**
  >
  > The /FILELIST parameter indicates that the file specified is a text file with one file name per line. Any white space at the start of a file is ignored. However, any white space at the end of the line is counted. Lines are delimited by any combination of carriage return characters, linefeed characters, or both.

  If you use this switch with the /UNICODE option, the CSCCMD tool creates the file list in Unicode text format.
- /DELETE: **Server****Share****Path**[/RECURSE] [/RECURSE2]
- Use this switch to delete a file, a directory, or a share from the local cache. To delete a directory or a share, you must make sure that the directory or the share is empty before you use this switch. If the directory or the share isn't empty, you can't delete the directory or the share. If the file is open, you can't delete the file. If you use this switch with the /RECURSE option, the CSCCMD tool only operates on the children of the path. If you use this switch with the /RECURSE2 option, the CSCCMD tool operates on the path and children of the path.
- /ISSERVEROFFLINE: **Server** - Use this switch to determine whether CSC considers a specific server to be offline.

  > ⓘ **Note**

Before you use this switch, you must open any share, file, or directory that is stored on the local cache for the server that you want to verify. If you do not do this, the CSCCMD command always reports that the server is online. Also, the server state that this command reports is the state that CSC recognizes. It is not the actual server state.

- /SETSPACE: **Bytes to Set** - Use this switch to specify the disk space in bytes that you want to allocate to temporary offline files. These temporary offline files are nonpinned, auto-cached files. This function works similarly to the function that is provided in the **Offline Files** dialog box.
- /CHECKDB [/QUICK] - Use this switch to examine the CSC database and to display any database error flags. If you use this switch with the /QUICK option, the CSCCMD tool skips the enumeration, and just displays the database errors.
- /EXTRACT[:**Server****Share**[**Path**]] /TARGET: **Path** [/RECURSE] [/ONLYMODIFIED] [/STOPONERROR] - Use this switch to extract a file, a directory, or a directory tree from the local cache. You can use the /TARGET option to specify the destination to which you want to extract the file or the directory. You can specify a destination folder that already exists, or you can specify a destination folder that doesn't already exist.

  > ⓘ **Note**
  >
  > If the destination folder that you specify does not already exist, the process automatically creates a folder that has the name that you specify.

  You can use the /ONLYMODIFIED option to extract only those files that have been modified offline. If you use the /STOPONERROR option, the extraction process stops whenever an error occurs during the extraction process.

  > ⓘ **Note**
  >
  > Because files in the offline cache use NTFS file system permissions, you must be an administrator on the local computer to use the /EXTRACT switch.

Current hotfixes for Windows 7 SP1 enterprise clients that have folder redirection enabled

Article • 03/24/2022 • 4 minutes to read

This article lists the hotfixes that are currently available for Windows 7 clients that are used in an Active Directory environment that makes use of data centralization, including folder redirection, offline files, and file server access.

Applies to: Windows 7 Service Pack 1
Original KB number: 2820927

Summary

In specific, the components of relevance here are:

- CSC (Client Side Caching, Offline Files)
- DFSC (Distributed File System client)
- Shell
- Folder Redirection
- Group Policy Preferences

For other components (client and server) like Srv.sys, mrxsmb.sys, rdbss.sys, ntfs.sys, dfssvc.exe, see the following up-to-date articles:

- List of currently available hotfixes for the File Services technologies in Windows Server 2008 and in Windows Server 2008 R2
- List of currently available hotfixes for the File Services technologies
- List of currently available hotfixes for Distributed File System (DFS) technologies in Windows Server 2008 and in Windows Server 2008 R2

This article contains a list of Microsoft Knowledge Base articles that describe the currently available fixes. Each section is divided into subsections for different component drivers:
DFS Namespace, Offline Files, Shell, Folder Redirection, and Group Policy Preferences.

> **Note**

The title of the latest fix might not represent the actual issue experienced, however LDR hotfixes do contain all previous fixes to that specific binary.

DFSN (DFS namespace) client component

Date added	Knowledge Base Article	Title	Why we recommend this hotfix	Hotfix type and availability
10. Feb. 2015	2916627 and 3000482	MS15-011: Vulnerability in Group Policy could allow remote code execution: February 10, 2015	This hotfix contains the most current version of dfsc.sys (6.1.7601.22917)	To apply this hotfix, you must have Windows 7 SP1, or Windows Server 2008 R2 SP1 installed and install both hotfixes.

Offline files components

Date added	Knowledge Base Article	Title	Why we recommend this hotfix	Hotfix type and availability
23/01/2014	2831206	DFS network path goes offline in Windows 7 or Windows Server 2008 R2 when Transparent Caching Group Policy setting is enabled	This hotfix contains the most current version of cscdll.dll and cscapi.dll.	To apply this hotfix, you must have Windows 7 SP1, or Windows Server 2008 R2 SP1 installed. Available for individual download.
23/05/2014	2967567	Cannot access DFS root when the DFS path is offline and you log on to a Windows-based computer for the first time	This hotfix contains the most current version of cscui.dll.	To apply this hotfix, you must have Windows 7 SP1, or Windows Server 2008 R2 SP1 installed. Available for individual download.

Shell component

Date added	Knowledge Base article	Title	Why we recommend this hotfix	Hotfix type and availability

Date added	Knowledge Base article	Title	Why we recommend this hotfix	Hotfix type and availability
09/05/2015	3009986	A copy or move operation is unsuccessful if a symbolic link is included	This hotfix contains the most current version of Shell32.dll.	To apply this hotfix, you must have Windows 7 SP1, or Windows Server 2008 R2 SP1 installed. Available for individual download.

Folder Redirection (fdeploy.dll)

Currently this binary is the latest available in SP1 for Windows 7.

Group Policy Preferences

Date added	Knowledge Base article	Title	Why we recommend this hotfix	Hotfix type and availability
07/04/2014	2953722	Drive Maps preferences are still displayed in Group Policy RSoP after they are removed or disabled	This hotfix contains the most current version of Gpprefcl.dll. (*)	To apply this hotfix, you must have Windows 7 SP1, or Windows Server 2008 R2 SP1 installed. Available for individual download.

(*) There's a more recent version in the GDR branch available (security hotfix deployed through Windows Update). Make sure that this hotfix AND all urgent/ critical fixes are installed. The version installed should be of a later date with version 6.1.760 1. 22 xxx and NOT 6.1.760 1. 18 xxx.

For Windows 8.1, install Offline Files network shares might not be available in Windows 8.1.

Under some circumstances, it might be necessary to reset the Offline Files database to reestablish the sync partnerships. These KB articles describe how to do it, or you can run the reg.exe command line to set the key followed by a reboot.

OS	Knowledge Base article	Reg.Exe command
XP	230738	REG ADD `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\NetCache /v FormatDatabase /t REG_DWORD /d 1 /f`

Folder redirection can move content when the folder redirection target is changed.

It's straight forward, except when moving between different names that are actually the same location - for example from NetBIOS (Network Basic Input/Output System) to FQDN name, or from server name to DFSN name.

To make sure that the move in these situations is successful, following group policy has to be set:

Verify Old and New folder redirection targets point to the same share before redirecting under `Windows Components\File Explorer` (or Windows Explorer)

Next of course Offline Files is involved because the redirected folder target is by default made offline available.

When the path is changed FR copies the data to the new location that can cause significant delays and corresponding network traffic (especially links with higher latency or when many users are migrated at the same time).

The bandwidth usage for this can't be controlled easily so an option is to copy the data on the backend to the new location with, for example, robocopy.

To make sure the minimum traffic is generated with the already copied data Folder Redirection will try to rename the data in the cache to the new location, rather than actually copying it. For this to work, you must set following registry key (via GPO preferences for example) for the user.

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ DWORD: FolderRedirectionEnableCacheRename: 1`

This key always has to be set.

Other data that is made available offline through admin assigning or manually making offline available is NOT automatically moved/ renamed.

Errors when you have a large "Folder Redirection" policy settings file in Windows

Article • 09/23/2021 • 4 minutes to read

This article provides a workaround for the problems that you may experience when you have a large "Folder Redirection" policy file.

Applies to: Windows 10 – all editions, Windows Server 2012 R2
Original KB number: 978098

Symptoms

Consider the following scenario:

- You set Folder Redirection policy settings for many folders in an environment.
- The folders are configured to use **Advanced Settings** when the user is a member of a group.
- The first time that you add all the groups to the list of folders, a large Folder Redirection policy settings file is created for many groups as expected.

In this scenario, you may encounter one or more of the following symptoms when you work with the large Folder Redirection policy settings file on a computer that is running Windows Vista, Windows Server 2008, Windows Server 2008 R2, or Windows 7.

Symptom 1

When you open the Folder Redirection policy settings, you find that the folders don't display the settings. Instead, the folders are displayed as **Not configured**.

Symptom 2

When you try to show the settings of the Folder Redirection policy in the Group Policy Management Console (GPMC), you receive the following error message in the **Folder Redirection Policy Details** section:

> An unknown error occurred while data was gathered for this extension. Details: FRSettingRead failed with -2147467259

> ⓘ **Note**
>
> For Symptom 1 and for Symptom 2, these symptoms occur on policies that are created and that are populated by using the Local Group Policy Editor on a computer that is running Windows Server 2003, Windows Server 2008, or a version of Windows that is newer than Windows Server 2008.

Symptom 3

When you try to apply the new Folder Redirection policy settings to a domain user account on a computer that is running Windows Vista or a newer version of Windows, the settings aren't applied. Additionally, you may receive the following error message in the Application log:

> Log Name: Microsoft-Windows-GroupPolicy/Operational
> Source: Microsoft-Windows-GroupPolicy
> Event ID: 7016
> Task Category: None
> Level: Error
> Keywords:
> User: SYSTEM
>
> Description:
> Completed Folder Redirection Extension Processing in **xxx** milliseconds.
>
> Event Xml:
> <Event xmlns="`http://schemas.microsoft.com/win/2004/08/events/event`">
> ...
> <EventData>
> <Data Name="ErrorCode">2147942413</Data>
> <Data Name="CSEExtensionName">Folder Redirection</Data>
> <Data Name="CSEExtensionId">{25537BA6-77A8-11D2-9B6C-0000F8080861}
> </Data>
> </EventData>
> </Event>

Cause

These issues occur because of two limitations in the system API that the Folder Redirection engine uses to read the .ini files from SYSVOL.

Cause of Symptom 1 and Symptom 2

- For an .ini file that was created in Windows Vista or in a newer version of Windows

  These issues occur because the Folder_Redirection section of the .ini files is larger than 32,767 characters. However, the limit for the combined SID list for all folders is 32,767 characters. This limit is encountered when the `GetPrivateProfileSection` API is used to read the section.

  > ⓘ **Note**
  >
  > If the SIDs typically have 48-50 characters, you can have about 670 SIDs in a policy for all folders before this issue occurs.

- For an .ini file that was created in Windows Server 2003

  These issues occur because the limit for the number of groups for each redirected folder in a policy is exceeded. This limit depends on the length of the SID string that represents the group and also on the length of the redirection path. For example, you can have about 230 groups for a single folder if a SID string is about 48-50 characters, and if the UNC path of the folder is 80 characters.

  > ⓘ **Note**
  >
  > - The aggregate size of all folders can exceed 32,767 characters.
  > - The first time that you open an existing policy, the settings may be converted to a newer format on a computer that is running Windows Vista or a newer version of Windows. This behavior may occur if the existing policy was created by using the Local Group Policy Editor in Windows Server 2003. This behavior also occurs when the policy settings are shown in the Settings view in the GPMC. Therefore, a policy might work by using the old .ini file format, depending on the settings. However, a policy might not work by using the new file format, depending on the settings.

Cause of Symptom 3

This issue occurs because of a limit of the `GetPrivateProfileString` API that is used to read this section.

The list of groups is stored as a string of SIDs in an .ini file. When the list exceeds 32,767 characters, this problem occurs. Each string that represents a SID in the .ini file is typically about 48-50 characters. Therefore, you can have around 300 entries for each redirected folder.

Workaround

To work around these problems, split the policy into smaller policies. Make sure that the total size of each policy file is smaller than the 32,767 character limit.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed at the beginning of this article.

More information

The Folder Redirection policy settings use a new .ini file format in Windows Vista and in newer versions of Windows to support new options when you apply the settings. This technology lets you redirect more folders compared to the Folder Redirection policy settings in Windows Server 2003.

For more information about the Folder Redirection feature, see General information about the Folder Redirection feature.

Folder redirection does not work correctly after you restart the computer

Article • 09/23/2021 • 4 minutes to read

This article provides workarounds for an issue where folder redirection doesn't work correctly after you restart computers.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 951049

Problem description

On a computer that is running Windows Server 2008 or Windows Vista, folder redirection is enabled. You log on immediately after you restart the computer. In this case, Windows Explorer tries to display the desktop before the Workstation service starts, and you experience one of the following problems:

- When you try to access redirected folders, you receive the following error message: ***servername***Username*sharename** is currently unavailable.
- The Documents, Pictures, Music, and Desktop folders are not visible.

Workaround

To work around this problem, use one of the following methods.

Method 1: Log off, and then log on again

Windows Explorer uses the Well-Known folder cache. The Well-Known folder cache is initialized during logon. When you log off and then log on again, Windows rebuilds the cache. At this point, you can apply Group Policy settings correctly. Additionally, the cache is populated correctly.

> **Note**
>
> For more information about Group Policy settings and about the Well-known folder cache, see the "**More information**" section.

Method 2: Wait for 12 minutes

The default update interval for the Well-Known folder cache is 12 minutes. To gain access to the redirected folders, wait for the 12-minute update interval to end.

Method 3: Decrease the update interval

You can change the registry to decrease the update interval for the Well-Known folder cache.

To have us fix this problem for you, go to the "Fix it for me" section. If you'd rather fix this problem yourself, go to the "Let me fix it myself" section.

Fix it for me

To fix this problem automatically, click the **Fix this problem** link. Then click **Run** in the **File Download** dialog box, and follow the steps in this wizard.

> ⓘ **Note**
>
> This wizard may be in English only; however, the automatic fix also works for other language versions of Windows.

> ⓘ **Note**
>
> If you are not on the computer that has the problem, you can save the automatic fix to a flash drive or a CD so that you can run it on the computer that has the problem.

Now go to the "Did this fix the problem?" section.

Let me fix it myself

> ⓘ **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the

registry, click the following article number to view the article in the Microsoft Knowledge Base: 322756 How to back up and restore the registry in Windows

You can decrease the update interval for the Well-Known folder cache by changing two registry values for the KnownFolderSettings subkey. These values control the intervals that are used to update the Well-Known folder cache, based on the success or failure of queries. By default, there is no KnownFolderSettings subkey. Instead, you must create this subkey. To create the KnownFolderSettings subkey and its values, follow these steps:

1. Click **Start**, click **Run**, type regedit, and then click **OK**.
2. Locate and then click the following registry key:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer`
3. On the **Edit** menu, point to **New**, and then click **Key**.
4. Type KnownFolderSettings, and then press ENTER.
5. Right-click KnownFolderSettings, point to **New**, click **DWORD Value**, and then type CachetimeoutSuccess.
6. Right-click CachetimeoutSuccess, and then click **Modify**.
7. In the **Value Data** field, type a value from 0 to 720000 milliseconds (ms).

   > **Note**
   >
   > The CachetimeoutSuccess registry value controls the time-out for cache entries that are populated successfully when the cache is built. We recommend that you set this value to the maximum value of 720000 ms (12 minutes) except when you have to configure the cache to repopulate the settings more frequently. Decreased values may cause an increase in processor and network load. (This increased load is associated with Windows Explorer.)

8. Right-click KnownFolderSettings, point to **New**, click **DWORD Value**, and then type CachetimeoutFailure.
9. Right-click CachetimeoutFailure, and then click **Modify**.
10. In the **Value Data** field, type a value from 0 to 720000 ms.

> **Note**

The CachetimeoutFailure registry value controls the time-out for cache entries that are not populated successfully when the cache is built. We recommend that you set this value to 60000 ms. When you do this, Windows Explorer tries to repopulate failed cache entries after 1 minute. This time frame is sufficient for the Workstation service to complete the initialization process.

Did this fix the problem?

Check whether the problem is fixed. If the problem is fixed, you are finished with this article. If the problem is not fixed, you can contact support.

More information

Windows Server 2008 and Windows Vista use the Well-Known folders feature to determine the location of folders in the user profile. By using this feature, Windows redirects Well-Known folders to other locations as needed. Specifically, Windows Explorer queries the Well-Known folder GUID. This query returns the actual folder location, whether on a hard disk drive or on a remote server.

Windows Explorer optimizes Well-Known folder lookups by caching the Well-Known folders and their locations. Queries are performed against the cache, and the location is then returned to the application or to Windows Explorer.

When you use folder redirection, you receive the folder redirection settings from Group Policy. This process cannot occur unless the Workstation service has started. If the Workstation service has not started, the Well-Known folder cache is unavailable. This causes queries for redirected folder locations to fail. Additionally, the cache remains unavailable until the next update. By default, this cache is updated every 12 minutes (after the cache is first initialized and built during logon).

Status

Microsoft has confirmed that this is a problem.

Folder Redirection fails to apply when redirected to mapped drive letter, instead of UNC path

Article • 09/23/2021 • 2 minutes to read

This article fixes an issue in which folder redirection fails to apply when redirected to mapped drive letter instead of UNC path.

Applies to: Windows 7 Service Pack 1
Original KB number: 2859465

Symptoms

Consider the following scenario:

- Home drive is configured for the users (for example: H:).
- Redirecting the folder to home drive using "Redirect to following location" and specify the drive letter (for example: H:\Documents) instead of using UNC path.
- The user is an administrator.

In this scenario, folder redirection fails to apply and the following event is logged:

> Log Name: Application
>
> Source: Microsoft-Windows-Folder Redirection
>
> Date: <DateTime>
>
> Event ID: 502
>
> Task Category: None
>
> Level: Error
>
> Keywords:
>
> User: Contoso\raj
>
> Computer: `TestPC.Contoso.com`
>
> Description:

> Failed to apply policy and redirect folder "Documents" to "H:\Documents".
>
> Redirection options=0x1001.
>
> The following error occurred: "Cannot create folder "H:\Documents"".
>
> Error details: "The system cannot find the path specified.

Cause

When an administrator logs on to Windows, the Local Security Authority (LSA) creates two access tokens. If LSA is notified that the user is a member of the Administrators group, LSA creates the second logon that has the administrator rights removed (filtered). Because LSA created the access tokens during two separate logon sessions, the access tokens contain separate logon IDs. The standard user access token is used to map the drive.

When the policy applies, it uses the highest token (admin token) and thus it fails to see the map drive.

Resolution

It's always recommended to use UNC path, not the drive map letter while redirecting a folder.

To resolve this issue, redirect the folder using UNC path instead of using map drive letter. You may use "Redirect to user's home directory" option if you want to redirect the folder to home drive.

Workaround

To work around this issue, use one of the following methods:

- Use "EnableLinkedConnections" registry. This value enables Windows to share network connections between the filtered access token and the full administrator access token for a member of the Administrators group. After you configure this registry value, LSA checks whether there's another access token that is associated with the current user session if a network resource is mapped to an access token. If LSA determines that there's a linked access token, it adds the network share to the linked location.

  To configure the EnableLinkedConnections registry value, follow these steps:

1. Click **Start**, type *regedit* in the **Start Search** box, and then press Enter.
2. Locate and then right-click the following registry subkey:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
3. Point to **New**, and then click **DWORD Value**.
4. Type *EnableLinkedConnections*, and then press Enter.
5. Right-click **EnableLinkedConnections**, and then click **Modify**.
6. In the **Value data** box, type *1*, and then click **OK**.
7. Exit Registry Editor, and then restart the computer.

> **Important**
>
> This workaround may make your system unsafe. Microsoft doesn't support this workaround. Use this workaround at your own risk.

- Disable UAC. Disabling UAC will stop splitting the token, but it's not recommended to disable UAC.

  Disabling User Account Control (UAC) on Windows Server

How to reinitialize the offline files cache and database in Windows XP

Article • 09/23/2021 • 2 minutes to read

This article provides two methods to reinitialize the offline files cache and database in Windows XP.

Applies to: Windows XP
Original KB number: 230738

Summary

The Offline Files (CSC or Client Side Caching) cache and database has a built-in capability to restart if its contents are suspected of being corrupted. If corruption is suspected, the Synchronization Wizard may return the following error message:

> Unable to merge offline changes on **server_name****share_name**. The parameter is incorrect.

More Information

Method 1

The Offline Files cache is a folder structure located in the %SystemRoot%\CSC folder, which is hidden by default. The CSC folder, and any files and subfolders it contains, should not be modified directly; doing so can result in data loss and a complete breakdown of Offline Files functionality.

If you suspect corruption in the database, then the files should be deleted using the Offline Files viewer. After the files are deleted out of the Offline Files viewer, a synchronization of files may then be forced using Synchronization Manager. If the cache still does not appear to function correctly, an Offline Files reset can be performed using the following procedure:

1. In **Folder Options**, on the **Offline Files** tab, press CTRL+SHIFT, and then click **Delete Files**. The following message appears:

   > The Offline Files cache on the local computer will be re-initialized. Any changes that have not been synchronized with computers on the network will be lost.

> Any files or folders made available offline will no longer be available offline. A computer restart is required.

Do you wish to reinitialize the cache?

2. Click Yes two times to restart the computer.

Method 2

Use Registry Editor

If you cannot access the **Offline Files** tab, use this method to reinitialize the Offline Files (CSC) cache on the system by modifying the registry. Use this method also to reinitialize the offline files database/client-side cache on multiple systems. Add the following registry subkey:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\NetCache`

Key Name: FormatDatabase
Key Type: DWORD
Key Value: 1

> ⓘ **Note**
>
> The actual value of the registry key is ignored. This registry change requires a restart. When the computer is restarting, the shell will re-initialize the CSC cache, and then delete the registry key if the registry entry exists.

> ⚠ **Warning**
>
> All cache files are deleted and unsynchronized data is lost.

Use Reg.exe

You can also automate the process of setting this registry value by using the Reg.exe command line editor. To do this, type the following command in the Reg.exe window:

Console

```
REG.EXE. REG ADD "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\NetCache"
/v FormatDatabase /t REG_DWORD /d 1 /f
```

Note

For specific steps to re-initialize the offline files cache and database in Windows Vista or Windows 7, click the following article number to view the article in the Microsoft Knowledge Base:
942974 On a Windows Vista or Windows 7-based client computer, you can still access offline files even though the file server is removed from the network.

Move the client-side caching (CSC) folder to a new location in Windows

Article • 09/23/2021 • 4 minutes to read

This article describes how to move the CSC folder in Windows. It also describes how to delete the old cache folder after you move the CSC cache folder to a new location.

Applies to: Windows 10, version 2004, Windows 10, version 1909, Windows 10, version 1709, Windows 7 Service Pack 1
Original KB number: 942960

> **Important**
>
> This article contains information about how to modify the registry. Make sure that you back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, see **How to back up and restore the registry in Windows**.

Why you can't use Cachemov.exe

The Cachemov.exe tool isn't supported in Windows Vista and later versions of Windows. When you try to use the Cachemov.exe tool to move the CSC folder in Windows Vista and later versions of Windows, you may receive the following error message:

> cachemov.exe - Ordinal Not Found
> The ordinal 51 could not be located in the dynamic link library CSCDLL.dll

> **Note**
>
> The CSC folder is the folder in which Windows Vista stores offline files.

The Cachemov.exe tool is used to move the CSC folder on a computer that contains one of the following operating systems:

- Windows Server 2003
- Windows XP
- Windows 2000 Server

Move the CSC folder

Typically, the offline files cache is located in the following directory: `%systemroot%\CSC`.

To move the CSC cache folder to another location in Windows Vista, Windows 7, Windows 8.1, and Windows 10, follow these steps:

1. Open an elevated command prompt. Select **Start** > **All Programs** > **Accessories**, right-click **Command Prompt**, and then select **Run as administrator**.

   If you're prompted for an administrator password or for a confirmation, type the password, or select **Allow**.

2. Type the following command, and then press ENTER:

   ```
   Console

   REG ADD "HKLM\System\CurrentControlSet\Services\CSC\Parameters" /v
   MigrationParameters /t REG_DWORD /d 1 /f
   ```

3. Type the following command, and then press ENTER:

   ```
   Console

   c:\windows\system32\migwiz\migwiz.exe
   ```

   > **Note**
   >
   > You may have to substitute a different drive letter, as appropriate for your situation.

4. In the Windows Easy Transfer Wizard, select the following options:

   a. Select **Start a New Transfer**.

   b. Select **My old computer**.

   c. Select **Use a CD, DVD or other removable media**.

   d. Select **External hard disk or to a network location**.

   e. Type a path where you want to save the Savedata.mig file, and then select **Next**.

   f. Select **Advanced options**.

g. In the **Select user accounts, files, and settings to transfer** dialog box, follow these steps:
   i. Clear all check boxes.
   ii. Under **System and program settings (all users)**, expand **Windows Settings** > **Network and Internet**, and then select the **Offline Files** check box.
   iii. Repeat the previous step for each user who is listed on the page.
   iv. Select **Next** to begin the transfer process.

Change the registry settings

> ⚠ **Warning**
>
> Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

Check the cache size that is used on the computer by following these steps:

1. In **Control Panel**, select **Network and Internet** > **Offline Files**.
2. Select the **Disk Usage** tab in the **Offline Files** box.

If the cache size is zero, you must change only the registry settings as given in the following list. Or, if the cache size is set to some value, follow all the steps.

1. Select **Start**, type *regedit* in the **Search** box, and then press ENTER.
2. Locate the following registry subkey, and then right-click it:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CSC`.
3. Right-click **CSC**, point to **New**, and then select **Key**.
4. Type *Parameters* in the name box.
5. Right-click **Parameters**, point to **New**, and then select **String Value**.
6. To name the new value, type *CacheLocation*, and then press ENTER.
7. Right-click **CacheLocation**, and then select **Modify**.
8. In the **Value data** box, type the name of the new folder in which you want to create the cache.

> ⓘ Note
>
> Use the Microsoft Windows NT format for the folder name. For example, if you want the cache location to be `d:\csc`, type `\??\d:\csc`.

9. Exit **Registry Editor**, and then restart the computer.

Continue the transfer process

1. At the elevated command prompt, type the following command, and then press ENTER: `c:\windows\system32\migwiz\migwiz.exe`.

2. In the Windows Easy Transfer Wizard, select the following options:
   a. Select **Continue a transfer in progress**.
   b. Select **No, I've copied files and settings to a CD, DVD, or other removable media**.
   c. Select **On an external hard disk or network location**.
   d. Type the path of the Savedata.mig file created in step 4e in the Move the CSC folder section.
   e. Map the user account on the old computer to the corresponding user account on the new computer.
   f. Select **Next** > **Transfer**.
   g. Restart the computer.

Delete the old cache

When all the files are moved, delete the old cache from a Windows Vista Release Candidate 1 (RC1) build by following these steps:

1. At the elevated command prompt, type the `takeown /r /f c:\windows\csc` command, and then press ENTER.

2. At the elevated command prompt, type the `rd /s c:\windows\csc` command, and then press ENTER.

> ⓘ Note
>
> The limitation of this method to delete the old cache is that Takeown.exe can only process paths that do not exceed the `MAX_PATH` (maximum length of a path). The

maximum length of a path is 260 characters. If this path length exceeds the `MAX_PATH`, the takeown command fails.

References

For more information about how to change the location of the CSC folder, see How to change the location of the CSC folder by configuring the CacheLocation registry value in Windows Vista.

Offline File Synchronization - In Windows 7 the "Work Offline/Work Online" option button disappears from Windows Explorer after an offline/online transition and the Client-Side Caching remains offline until the next restart of the computer

Article • 09/23/2021 • 3 minutes to read

This article provides a solution to solve issues where the Work Offline/Work Online option button disappears from Windows Explorer after an offline/online transition and the Client-Side Caching remains offline until the next restart of the computer.

Applies to: Windows 7 Service Pack 1
Original KB number: 2512089

Symptoms

You have Windows 7 configured for offline file synchronization to synchronize content from network shares and have it available offline. Users notice that Windows 7 changes usually to offline mode; however Windows 7 does not switch back to online mode automatically after the network becomes available. Synchronization of the UNC path is not possible, and in the Sync Center no information is available for the offline file synchronization partnership.

If the user accesses network resources in Windows Explorer, some network resources are online and accessible; however when the user tries to access resources that have been made available offline, the offline content is displayed from the Client-Side Caching. The user can create new files and change existing files, but these files remain in the local cache.

You provide a file share and subfolders for every user like in the following example:

\\ServerName\ShareName$\dir1\dir2

A user with the appropriate permissions can access subfolders dir1 and dir2 but do not have permissions to view the content of the share ShareName$.

Cause

This behavior is caused by the way Windows Vista and Windows 7 handle remote file operations. The UNC path is parsed and every part is checked for availability. In the case described in the sections above, Windows Vista or Windows 7 checks for the prefix \\ServerName. If this is successful, it checks if the \\ShareName$\ is available. Due to missing access rights on this level, the remote file operation fails and the Client-Side Caching (CSC) provides files from the offline content if the UNC path was made available offline.

> ⓘ **Note**
>
> if you are using DFS Namespace (AD integrated or stand alone) \\domain\folder1\folder2 CSC will also check folder1 and folder2 on the DFS Namespace server.

Resolution

To solve this issue with the offline file synchronization ensure that all parts of an UNC path are accessible by a user. On an UNC path like \\ServerName\ShareName$\dir1\dir2 (where ServerName can be a file server or DFSN server) the following permissions are required on ShareName$ when the user synchronizes the subfolder dir1:

Share level (SMB) Permissions for the offline files share ShareName$:

User Account	**Default Permissions**	**Minimum permissions required**
Everyone	Read	No Permissions
Security group of users needing to put data on share.	N/A	Change

In this example, Everyone is removed from the share permissions and a global group containing the user account is used to set share level permissions.

NTFS permissions needed for the root folder ShareName$ for offline file synchronization:

User Account	**Minimum Permissions Required**
Creator Owner	Full Control, Subfolders and Files Only

User Account	Minimum Permissions Required
Administrator	None
Security group of users that need to put data on share	List Folder/Read Data - This Folder, Subfolders and Files
Everyone	No Permissions
Local System	Full Control, This Folder, Subfolders and Files

On the subfolders \dir1 and \dir2, the following permissions are required: NTFS permissions needed for the folders dir1 and dir2 for offline file synchronization:

User Account	Default Permissions	Minimum permissions required
%Username%	N/A	Read, Write
Local System	Full Control	Full Control
Administrators	No Permissions	No Permissions
Everyone	No Permissions	No Permissions

More information

In Windows Vista and Windows 7, all remote file system access requests are channeled by the Multiple UNC Provider (MUP). MUP redirects the request to a network redirector (the UNC provider) that is capable to handle the remote file system request. For example, for SMB requests MUP redirects the request to the network provider LanmanWorkstation (ntlanman.dll). LanmanWorkstation calls the Workstation Service (svchost.exe) that calls the network redirector (mrxsmb.sys).

MUP performs a prefix resolution operation (IOCTL_REDIR_QUERY_PATH) request to the network redirector that is registered with MUP and capable for the type of request. This prefix resolution operation parses the UNC path and checks every part for availability. If the return message from the prefix resolution is STATUS_LOGON_FAILURE or STATUS_ACCESS_DENIED, the request fails and MUP states the UNC path as not accessible.

The Client-Side Caching intercepts requests that are channeled to the network redirector. If the prefix resolution operation fails like described in the section above, CSC provides content from the local cache if the UNC path was made available offline before.

The behavior is outlined in detail on the following links:

- Support for UNC Naming and MUP
- IOCTL_REDIR_QUERY_PATH IOCTL
- Basic Architecture of a Network Redirector

Intranet site is identified as an Internet site when you use an FQDN or an IP address

Article • 09/23/2021 • 9 minutes to read

This article provides a workaround for an issue where an Intranet site is identified as an Internet site when you use a fully qualified domain name (FQDN) or an IP address.

Applies to: Windows 10 - all editions
Original KB number: 303650

Symptoms

When you access a local area network (LAN), an intranet share, or an intranet Web site by using an Internet Protocol (IP) address or a FQDN, the share or Web site may be identified as in the Internet zone instead of in the Local intranet zone. For example, this behavior may occur if you access shares or Web sites with Microsoft Internet Explorer or Windows Internet Explorer, with Microsoft Windows Explorer, with a command prompt, or with a Windows-based program when you use an address in any one of the following formats:

- `\\Computer.childdomain.domain.com\Share`
- `http://computer.childdomain.domain.com`
- `\\157.54.100.101\share`
- `file://157.54.100.101/share`
- `http://157.54.100.101`

This behavior can occur regardless of whether any or all of the following settings are configured:

- In Microsoft Internet Explorer or in Windows Internet Explorer, you have added the FQDN (or *.domain.com) or the IP address (or the address range) to the **Do not use proxy server for addresses beginning with** box under the **Exceptions** section in the **Proxy Settings** dialog box.

  > **Note**
  >
  > To locate the **Proxy Settings** dialog box in Internet Explorer, click **Tools**, click **Internet Options**, click **Connections**, and then click **Proxy Settings**.

- You have selected the **Bypass proxy server for local addresses** check box that is on the **Local Area Network (LAN) Settings** dialog box.

  > ⓘ Note
  >
  > To locate the **Local Area Network (LAN) Settings** dialog box in Internet Explorer, click **Tools**, click **Internet Options**, click **Connections**, and then click **Local Area Network (LAN) Settings**.

- You have selected the **Include all sites that bypass the proxy server** and **Include all network paths (UNCs)** check boxes on the **Local intranet** dialog box.

  To locate the **Local intranet** dialog box in Internet Explorer, click **Tools**, click **Internet Options**, click **Security**, and then click **Local intranet**.

This behavior can cause Internet Explorer to prompt you for credentials when you access the intranet Web sites that require authentication. Or you may be prompted or prevented from opening files on an intranet Web site or Universal Naming Convention (UNC) share in programs that use the Internet Explorer Security Manager to determine whether a file is located in a trusted security zone. For example, you may receive the following error message when you try to open an Access database (.mdb) file on a local intranet share (by using the FQDN or IP address) with Access 2002:

> Microsoft Access cannot open this file.
> This file is located outside your intranet or on an untrusted site. Microsoft Access will not open the file due to potential security problems.
> To open the file, copy it to your computer or an accessible network location.

> ⓘ Note
>
> Windows Server 2003 includes a new, optional component named Internet Explorer Enhanced Security Configuration. This component assigns all intranet Web sites and all UNC paths that are not explicitly listed in the Local intranet zone to the Internet zone. By default, the Internet zone uses the High security level. Therefore, you may experience these symptoms when you access intranet Web sites and UNC paths by using the NetBIOS name. For example, if you use `http://server` or \\server\share, or when you use the IP address or FQDN, you may experience these symptoms.

For more information about Internet Explorer Enhanced Security Configuration, see FAQ about Internet Explorer Enhanced Security Configuration (ESC).

Cause

This behavior may occur if an FQDN or IP address contains periods. If an FQDN or IP address contains a period, Internet Explorer identifies the Web site or share as in the Internet zone.

Workaround

To work around this issue, add the appropriate IP address range or fully qualified domain names (FQDNs) to your local intranet. Or change the security level of the Internet zone. On user authentication option, change from automatic logon only on Intranet zone to automatic logon with current user name and password.

If you are using Internet Explorer's Enhanced Security Configuration with Windows Server 2003, and you use the NetBIOS name to access intranet sites, use any of the following methods to work around this issue:

- Add the sites to the Local intranet zone. To add a site to the Local intranet zone, open the site in Internet Explorer, click **File**, point to **Add this site to**, click **Local intranet zone**, click **Add** in the **Local intranet** dialog box, and then click **Close**.
- Add the sites to the Trusted sites zone. To add a site to the Trusted sites zone, open the site in Internet Explorer, click **File**, point to **Add this site to**, click **Trusted sites zone**, click **Add** in the **Trusted sites** dialog box, and then click **Close**.
- Turn off Enhanced Security Configuration. You must be an administrator to turn off Enhanced Security Configuration. You can turn off Enhanced Security Configuration for users (such as Limited Users and Restricted Users) and leave it on for administrators. To turn off Enhanced Security Configuration for users, open **Control Panel**, click **Add or Remove Programs**, click **Add/Remove Windows Components**, click **Internet Explorer Enhanced Security Configuration**, click **Details**, click **Users**, click **OK**, click **Next**, click **Finish**, and then restart Internet Explorer to apply the new settings.

Administrators can use client settings or server settings to add the appropriate IP address range or FQDNs to the Local intranet. For example, administrators can use TCP/IP suffixes, add *.domain.com, or add the appropriate IP address range to the **Local intranet sites** zone in Internet Explorer on the client. On the server, administrators can use a proxy automatic configuration script. The following workaround adds *.domain.com or the appropriate IP address range to the Local intranet sites zone in Internet Explorer for all the client computers.

Users

To work around this behavior, each user must add *.domain.com or the appropriate IP address range to the **Local Intranet Sites** dialog box:

1. In Internet Explorer, click **Tools**, and then click **Internet Options**.
2. On the **Security** tab, click **Local intranet**, and then click **Sites**.
3. Click **Advanced**, and then type *.domain.com, or an IP address range (for example, 157.54.100-200.*) in the **Add this Web site to the zone** box, where `domain.com` is your company and top-level domain names.
4. Click **Add**, click **OK**, click **OK**, and then click **OK** again to close the **Internet Options** dialog box.
5. Restart the computer.

Administrators

> **ⓘ Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

Administrators can deploy this setting by making the following changes to the registry:

1. For each domain that should be included in the Local intranet zone, add a `domain.com` key to the appropriate registry key under either **HKEY_CURRENT_USER** (for a currently logged-on user only) or **HKEY_LOCAL_MACHINE** (for all users on the local computer):

    - `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains` (For 32-bit versions of Internet Explorer or 64-bit versions of Internet Explorer on 64-bit versions of Windows XP or Windows Server 2003, if Enhanced Security Configuration is turned off.)

    - `Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains` (For 32-bit versions of Internet Explorer on 64-bit versions of Windows XP or 64-bit versions of Windows Server 2003, if Enhanced Security Configuration is turned off.)

- `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ESCDomains` (For Internet Explorer on 32-bit versions of Windows Server 2003, or the 64-bit version of Internet Explorer on 64-bit versions of Windows Server 2003, if Enhanced Security Configuration is turned on.)

- `Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ESCDomains` (For the 32-bit version of Internet Explorer on 64-bit versions of Windows Server 2003, if Enhanced Security Configuration is turned on.)

> ⓘ **Note**
>
> By default, security zones settings are stored in the **HKEY_CURRENT_USER** registry key. Because this key is dynamically loaded for each user, the settings for one user do not affect the settings of another. Only the local machine settings will be used if the **Security Zones: Use only machine settings** setting is enabled in group policy or the Security_HKLM_only DWORD value is set to 1 in the following key:
> `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings`
> With this policy setting enabled, only machine settings will be used instead of user settings.

2. Add a DWORD value named the asterisk character (*) to the `domain.com` key and set it to 1.

3. For each IP address range that must be included in the Local intranet zone, add a Range**x** key (where x is 1, 2, 3, and so on) to the following registry key under **HKEY_CURRENT_USER** (for a currently logged-on user only) or **HKEY_LOCAL_MACHINE** (for all users on the local computer):

   - `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Ranges` (For 32-bit versions of Internet Explorer or 64-bit versions of Internet Explorer on 64-bit versions of Windows XP or Windows Server 2003.)

   - `Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Ranges` (For 32-bit versions of Internet Explorer on 64-bit versions of Windows XP or 64-bit versions of Windows Server 2003.)

> ⓘ **Note**
>
> By default, security zones settings are stored in the **HKEY_CURRENT_USER** registry key. Because this key is dynamically loaded for each user, the settings for one user do not affect the settings of another. Only the local machine settings will be used if the **Security Zones: Use only machine settings** setting is enabled in group policy, or if the Security_HKLM_only DWORD value is set to 1 in the following key:
> `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings`
> With this policy setting is enabled, only machine settings will be used instead of user settings.

4. Add a DWORD value named the asterisk character (*) to the Range**x** key and set it to 1.

5. Add a String value named *:Range* (the colon character followed by the word Range) to the Range**x** key, and then set it to the IP address range (for example, 157.54.100-200.*).

> ⓘ **Note**
>
> Administrators can deploy settings in an Active Directory environment.

For more information about how to do so, see How to set advanced settings in Internet Explorer by using Group Policy objects.

> ⓘ **Important**
>
> This workaround does not work for UNC or file:// addresses that use an IP address. For example, Internet Explorer identifies \\157.54.100.101\share, or file://157.54.100.101/share, as being in the Internet zone, even if you add the appropriate IP address range to the Local Intranet Sites list. In this case, you must use a file:// URL that has the NetBIOS name (for example, **\\server\share**) for the site to be identified in the Local intranet zone. Also, some applications may not be able to open files by using an http:// address even if the Web site is on your LAN and you use the NetBIOS name (for example, `http://server`). For example, Access 2002 cannot open files from http:// addresses. If you try to open an Access database file (.mdb) on an intranet Web site by using either the IP address, FQDN, or NetBIOS name, Access 2002 will incorrectly report that the file is outside your

intranet or on an untrusted site by displaying the error message in the **Symptoms** section of this article.

Status

This behavior is by design.

Change the default maximum transmission unit (MTU) size settings for PPP connections or for VPN connections

Article • 09/23/2021 • 4 minutes to read

This article describes how to edit the registry to change the default maximum transmission unit (MTU) size settings for Point-to-Point Protocol (PPP) connections or for virtual private network (VPN) connections.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 826159

Summary

Windows Server 2003, Windows 2000, and Windows XP use a fixed MTU size of 1500 bytes for all PPP connections and use a fixed MTU size of 1400 bytes for all VPN connections. This is the default setting for PPP clients, for VPN clients, for PPP servers, or for VPN servers that are running Routing and Remote Access.

PPP connections are connections such as modem connections, Integrated Services Digital Network (ISDN) connections, or direct cable connections over null serial cable or over parallel cable. VPN connections are Point-to-Point Tunneling Protocol (PPTP) connections or Layer 2 Tunneling Protocol (L2TP) connections.

> ⓘ **Note**
>
> Use the methods in this article to edit the registry to modify the MTU size settings. If you experience any problems or any performance-related issues after you modify the MTU size settings, remove the registry keys that you added.

Change the MTU settings for PPP connections

To change the MTU settings for PPP connections, add the **ProtocolType** DWORD value, the **PPPProtocolType** DWORD value, and the **ProtocolMTU** DWORD value to the following registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ndiswan\Parameters\Protocols\0`

To do so, follow these steps.

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Window**.

1. Click **Start**, click **Run**, type *regedit* in the **Open** box, and then click **OK**.
2. Locate and then click the following subkey in the registry:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters`
3. Add a **Protocols** subkey (if it does not already exist):
   a. On the **Edit** menu, point to **New**, and then click **Key**.
   b. Type *Protocols*, and then press ENTER.
4. Add a **0** (zero) subkey to the **Protocols** subkey:
   a. Click the **Protocols** subkey that you created step 3.
   b. On the **Edit** menu, point to **New**, and then click **Key**.
   c. Type 0 (zero), and then press ENTER.
5. Click the **0** subkey that you created in step 4.
6. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
7. In the **Value data** box, type *ProtocolType*, and then click **OK**.
8. On the **Edit** menu, click **Modify**.
9. In the **Value data** box, type *800*, make sure **Hexadecimal** is selected under **Base**, and then click **OK**.
10. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
11. Type *PPPProtocolType*, and then press ENTER.
12. On the **Edit** menu, click **Modify**.
13. In the **Value data** box, type *21*, make sure **Hexadecimal** is selected under **Base**, and then click **OK**.

14. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
15. Type *ProtocolMTU*, and then press ENTER.
16. On the **Edit** menu, click **Modify**.
17. Under **Base**, click **Decimal**, type the MTU size that you want in the **Value data** box, and then click **OK**.
18. Quit Registry Editor.
19. Restart your computer.

Change the MTU settings for VPN connections

To change the MTU settings for VPN connections, add the **ProtocolType** DWORD value, the **PPPProtocolType** DWORD value, and the **TunnelMTU** DWORD value to the following registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ndiswan\Parameters\Protocols\0`

To do so, follow these steps.

> **ⓘ Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

1. Click **Start**, click **Run**, type *regedit* in the **Open** box, and then click **OK**.
2. Locate and then click the following subkey in the registry:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters`
3. Add a **Protocols** subkey (if it does not already exist):
   a. On the **Edit** menu, point to **New**, and then click **Key**.
   b. Type *Protocols*, and then press ENTER.
4. Add a **0** (zero) subkey to the **Protocols** subkey:
   a. Click the **Protocols** sub key that you created in step 3.

b. On the **Edit** menu, point to **New**, and then click **Key**.
c. Type *0* (zero), and then press ENTER.

5. Click the **0** subkey that you created in step 4.
6. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
7. In the **Value data** box, type *ProtocolType*, and then click **OK**.
8. On the **Edit** menu, click **Modify**.
9. In the **Value data** box, type *800*, make sure **Hexadecimal** is selected under **Base**, and then click **OK**.
10. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
11. Type *PPPProtocolType*, and then press ENTER.
12. On the **Edit** menu, click **Modify**.
13. In the **Value data** box, type *21*, make sure **Hexadecimal** is selected under **Base**, and then click **OK**.
14. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
15. Type *TunnelMTU*, and then press ENTER.
16. On the **Edit** menu, click **Modify**.
17. Under **Base**, click **Decimal**, type the MTU size that you want in the **Value data** box, and then click **OK**.
18. Quit Registry Editor.
19. Restart your computer.

References

For more information about PPP, see Request for Comments (RFC) 1548. To do so, see RFC 1548.

CMAK-based VPN client doesn't work after an in-place upgrade to Windows 10

Article • 09/23/2021 • 2 minutes to read

This article helps fix an issue where CMAK-based VPN client does not work after Windows is upgraded to Windows 10 - all editions.

Applies to: Windows 10 - all editions
Original KB number: 4052854

Symptom

After you upgrade Windows to Windows 10, version 1703 (Creators Update), Windows 10, version 1709 (Fall Creators Update), Windows 10, version 1803, Windows 10, version 1809, or Windows 10, version 1909, you can't start a Connection Manager Administration Kit (CMAK)-based Virtual Private Network (VPN) client.

Resolution

To fix this issue, reinstall the CMAK-based VPN package.

Default gateway route doesn't appear in the Routing Table after you re-add a Routing and Remote Access interface

Article • 08/01/2022 • 2 minutes to read

This article provides a solution to an issue where default gateway route doesn't appear in the Routing Table.

Applies to: Windows Server - all editions
Original KB number: 816905

Symptoms

When you add a network interface to a remote access server in the Routing and Remote Access utility, a default route for that interface may not appear in the routing table.

Cause

This issue may occur if both of the following conditions are true:

- You remove a network interface from the remote access server.
- You re-add that network interface to the remote access server.

To work around this issue, use one of the following methods.

Workaround 1: Manually add the default route for the Interface

Use the Route Add command to manually add the default route for the network interface that you added.

1. Click **Start**, click **Run**, type *cmd* in the **Open** box, and then click **OK**.

2. Type route print, and then press ENTER to view the routing table. Note the interface number of the network interface that you re-added.

3. Type the following command, and then press ENTER route add 0.0.0.0 mask 0.0.0.0 **gateway IP** metric **30** if **Interface number**
   where **gateway IP** is the IP address of the default gateway for this interface, and

where **Interface number** is the number that corresponds to the network interface that you added (for example, 2). For example, if your default gateway IP address is 192.168.1.1 and the interface number is 2, type the following command, and then press ENTER:

```
Console

route add 0.0.0.0 mask 0.0.0.0 192.168.1.1 metric 30 if 2
```

4. Type route print to verify that the new default route appears in the routing table.
5. Close the command prompt.

Workaround 2: Restart the remote access service

Restart the remote access service. The default route for the re-added network interface is added to the Windows routing table.

1. Start the Routing and Remote Access utility.
2. Under **Routing and Remote Access**, right-click the server where you re-added the network interface, point to **All Tasks**, and then click **Restart**.

Workaround 3: Restart the server

Restart the remote access server. The default route for the re-added network interface is added to the Windows routing table.

DirectAccess clients can connect over Teredo but not through IP-HTTPS

Article • 09/23/2021 • 3 minutes to read

This article describes an issue that prevents DirectAccess clients from connecting by using IP-HTTPS even though they can connect over Teredo.

Applies to: Windows Server 2012 R2, Windows 10 – all editions
Original KB number: 2980660

Symptoms

DirectAccess clients can connect over Teredo, but may be unable to connect by using IP-HTTPS.

When you run the netsh interface http show interface command, the output is as follows:

> Error: 0x643
> Translates to: Fatal error during installation.
>
> Error: 0x34
> Translates to: Interface creation failure.

Cause

> Error: 0x643
> Translates to: Fatal error during installation.
>
> 0x643 translates to:
> ERROR_INSTALL_FAILURE
> #Fatal error during installation.
>
> Error: 0x34
> Translates to : Interface creation failure.
>
> 0x34 translates to:
> ERROR_DUP_NAME
> # You were not connected because a duplicate name exists on
> # the network. If joining a domain, go to System in Control

> # Panel to change the computer name and try again. If joining
> # a workgroup, choose another workgroup name.

The reasons for these error codes are the same. Both error codes indicate a pre-existing setting or interface that conflicts with the currently applied IP-HTTPS configuration.

Possible causes for this issue include the following:

- Duplicate or corrupted IP-HTTPS interface in device manger.
- Corrupted or invalid ACL for IP-HTTPS binding (this is server-side issue).
- IPv6 Transition Adapters are disabled, or all IPv6 is disabled.

  > ⓘ **Note**
  >
  > If IPv6 isn't selected on the NIC, but the DisabledComponents registry key has not been set, then you can ignore this possible cause.

Resolution

If there are corrupted or duplicate IP-HTTPS interfaces

- Clear all stale IP-HTTPS interfaces from Device Manager:

  1. Make sure that you're looking at the hidden and ghost devices.
     - Set devmgr_show_nonpresent_devices=1.
     - Open devmgmt.msc.
     - Select show hidden devices.

     > ⓘ **Note**
     > - In Windows 8, the IP-HTTPS interface will appear under Network Adapters.
     > - In Windows 8.1, there will also be a "Microsoft IPv4 IPv6 Transition Adapter Bus" under Software Devices that might need to be reinstalled.
     > - *Do not* remove the Transition adapter on a DirectAccess server, because this all DirectAccess traffic to cease.

2. Reset the IP-HTTPS interface on the machine, and then reapply the configuration (GPO).

- Clear the stale or duplicate entries from the registry:

  1. Delete the following subkeys:

     `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Tcpip\v6Transition\IPHTTPS`

     `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Tcpip\v6Transition\IPHTTPSProfiles`

  2. Restart the IPHLPSVC, and then restart the computer while connected to the corporate LAN to apply Group Policy settings again.

- A hotfix has been released to address this issue.

  2966807 Randomly you cannot connect to the DirectAccess server by using the IP-HTTPS adapter in Windows 8.1 and Windows Server 2012 R2

If there's server-side IP-HTTPS creation failure

- Back up and then delete the following registry key:

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\HTTP\Parameters\UrlAclInfo`

- Delete the following keys:

  - `https://+:443/C574AC30-5794-4AEE-B1BB-6651C5315029/`
  - `https://+:443/sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}/`

    > **Note**
    >
    > Be aware that this is a *server-side* fix.

If IPv6 or only IPv6 Transition Adapters are disabled

If IPv6 is disabled make sure to enable it back.

If the DisabledComponents registry key is set under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6`, then delete it, or make

sure that transition adapters aren't being disabled.

For more information about this, go to the following article at the Microsoft Knowledge Base:

929852 How to disable IPv6 or its components in Windows

More information

DirectAccess connectivity methods

DirectAccess clients use multiple methods to connect to the DirectAccess server, which enables access to internal resources. Clients can use either Teredo, 6to4, or IP-HTTPS to connect to DirectAccess. This also depends on how the DirectAccess server is configured.

When the DirectAccess client has a public IPv4 address, it will try to connect by using the 6to4 interface. However, some ISPs give the illusion of a public IP Address. What they provide to end users is a pseudo public IP address. This means that the IP address received by the DirectAccess client (a data card or SIM connection) might be an IP from the public address space but that it's actually located behind one or more NATs.

When the client is behind a NAT device, it will try to use Teredo. Many businesses such as hotels, airports, and coffee shops don't allow Teredo traffic to traverse their firewall. In such scenarios, the client will fail over to IP-HTTPS. IP-HTTPS is built over an SSL (TLS) TCP 443-based connection. SSL outbound traffic will most likely be allowed on all networks.

Having this in mind, IP-HTTPS was built to provide a backup connection that is reliable and always reachable. A DirectAccess client will make use of this when other methods (such as Teredo or 6to4) fail.

More information about transition technologies can be found at IPv6 transition technologies .

DirectAccess clients may be unable to connect with error 0x80092013

Article • 09/23/2021 • 6 minutes to read

This article provides help to solve an issue where DirectAccess clients aren't able to connect to DirectAccess Server by using Internet Protocol over Secure Hypertext Transfer Protocol (IP-HTTPS) connections.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2980672

Symptoms

DirectAccess clients may be unable to connect to DirectAccess Server by using IP over IP-HTTPS connections because the revocation check fails.

The output of the command netsh interface http show interface will display the following error:

> Error: 0x80092013
>
> Translates to: CRYPT_E_REVOCATION_OFFLINE
> # The revocation function was unable to check revocation because the revocation server was offline.

Cause

This error may occur for one of the following reasons:

1. The CRL location (CDP) is unreachable.
2. The CRL location (CDP) is unpublished.
3. The CRL has expired and a new one was not published.
4. The CRL is reachable but the client is picking from an old cache.

Resolution

If the CRL location (CDP) is unreachable, then verify that the CRL is downloadable from the system context by following these steps:

1. Determine whether the connectivity issue is being caused by the Proxy Settings. To determine this you can query by using the follow registry values:

   - cmd.exe /c reg query `HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings` /v ProxyEnable
   - cmd.exe /c reg query `HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings` /v ProxyServer
   - cmd.exe /c reg query `HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings` /v ProxyOverride
   - cmd.exe /c reg query `HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings` /v AutoConfigURL
   - cmd.exe /c reg query `HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings` /v ProxyEnable
   - cmd.exe /c reg query `HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings` /v ProxyServer
   - cmd.exe /c reg query `HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings` /v ProxyOverride
   - cmd.exe /c reg query `HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings` /v AutoConfigURL

   a. If the **ProxyEnable** value equals 1 in either. Default or S-1-5-18 then it means DO NOT **Automatically Detect Settings**. This means that connections are made only by using the proxy defined in **ProxyServer** or **AutoConfigURL**.
   b. If the ProxyEnable value equals 0, it means **Automatically Detect Settings**. Therefore you cannot change the Value in the registry to make DA work as the HKU\<UserSID> hive is the dump for the HKCU hive. Any changes that you made to HKU will be overwritten every time that the **System Service** is active. To change this setting, you must start Internet Explorer or CMD.exe under the **System Account** (NT AUTHORITY\System). To do this, from an elevated **Command Prompt** run:

- psexec.exe -s -i cmd.exe /c reg add `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings` /v ProxyEnable /t REG_DWORD /d 0 /f
  - CRL Location could be unreachable for one of the following reasons:

  a. System context proxy is applied but unreachable and requires user authentication.

  b. Hotspot logon is pending.

  c. CRL Location is unavailable on the Internet.

  d. CRL Location requires authentication before access is granted.

  e. CRL Location is reachable. But the CRL files are not allowed to be served.
  - In this case, check **File System Permissions** on the CRL and Delta CRL files.
  - Ensure that **DoubleEscaping** is enabled for the CDP location:
    - Set-WebConfiguration -Filter system.webServer/security/requestFiltering -PSPath 'IIS:\Sites<SiteName> -Value @{allowDoubleEscaping=$true}

2. If the CRL location (CDP) is unpublished follow these steps:

   a. Click **Start**, point to **Administrative Tools**, and then click **Certification Authority**.

   b. In the console tree, right-click **corp-DC1-CA**, and then click **Properties**.

   c. Click the **Extensions tab**, and then click **Add**.

   d. In **Location**, type `http://\<Public-IIS-URL>/crld/` (WAN URL required Internet Access)

   e. In **Variable**, click <CAName>, and then click **Insert**.

   f. In **Variable**, click <CRLNameSuffix>, and then click **Insert**.

   g. In **Variable**, click <DeltaCRLAllowed>, and then click **Insert**.

   h. In **Location**, type .crl at the end of the Location string, and then click **OK**.

   i. Select **Include** in CRLs. Clients use this to find Delta CRL locations. Select **Include** in the CDP extension of issued certificates, and then click **OK**. Then click **Add**.

   j. In **Location**, type \<IIS-ServerName>\crldist$\ (Internal Location used by the Certification Authority to publish to and by IIS to serve clients.)

   k. In **Variable**, click <CAName>, and then click **Insert**.

   l. In Variable, click <CRLNameSuffix>, and then click **Insert**.

   m. In Variable, click <DeltaCRLAllowed>, and then click **Insert**.

   n. In Location, type .crl at the end of the string, and then click **OK**.

   o. Select **Publish CRLs** to this location and **Publish Delta CRLs** to this location, and then click **OK**.

   p. Click yes to restart Active Directory Certificate Services.

   q. Close the Certification Authority console.

3. If the CRL has expired follow these steps:

   - Republish the CRL
     - Certutil -crl

4. If the CRL is reachable but the client is picking from an old cache, follow these steps:

   Clear the client Caches

   a. TVO (Time Validated objects)

      - Certutil -setreg chain\ChainCacheResyncFiletime @now

   b. URL Cache

      - Certutil -urlcache * delete

More information

DirectAccess Connectivity Methods

DirectAccess clients use multiple methods to connect to the DirectAccess server. This enables access to internal resources. Clients have the option to use either Teredo, 6to4, or IP-HTTPS to connect to DirectAccess. This also depends on how the DirectAccess server is configured.

When the DirectAccess client has a public IPv4 address, it will try to connect by using the 6to4 interface. However, some ISPs give the illusion of a public IP Address. What they provide to end users is a pseudo public IP address. What this means is that the IP address received by the DirectAccess client (a data card or SIM connection) might be an IP from the public address space, but in reality is behind one or more NATs.

When the client is behind a NAT device, it will try to use Teredo. Many businesses such as hotels, airports, and coffee shops do not allow Teredo traffic to traverse their firewall. In such scenarios, the client will fail over to IP-HTTPS. IP-HTTPS is built over an SSL (TLS) TCP 443-based connection. SSL outbound traffic will most likely be allowed on all networks.

Having this in mind, IP-HTTPS was built to provide a backup connection that is reliable and always reachable. A DirectAccess client will use this when other methods (such as Teredo or 6to4) fail.

More information about transition technologies can be found at IPv6 transition technologies.

Certificate Revocation Lists

Certificate revocation lists (CRLs) are used to distribute information about revoked certificates to individuals, computers, and applications that try to verify the validity of certificates. CRLs are complete, digitally signed lists of unexpired certificates that have been revoked. The CRL is retrieved by clients who can then cache the CRL (based on the configured lifetime of the CRL) and use it to verify certificates presented for use. By default, the CRL is published in two locations by a Microsoft Enterprise CA:

- `http://CAName/certenroll/CRLName`
- LDAP:///CN=CAName,CN=CAComputerName,CN=CDP,CN=PublicKeyServices,CN=Services,CN=Configuration,DC=ForestRootDomain,DC=TL

Basic Certificate Chain Validation

When CryptoAPI builds and validates a certificate chain, three distinct phases occur:

1. All possible certificate chains are built by using locally cached certificates. If none of the certificate chains end in a self-signed certificate, CryptoAPI then selects the best possible chain and tries to retrieve issuer certificates specified in the authority information access extension to complete the chain. This process is repeated until a chain to a self-signed certificate is built.
2. For each chain that ends in a self-signed certificate in the trusted root store, revocation checking is performed.
3. Revocation checking is performed from the root CA certificate down to the evaluated certificate.

More information about certificate revocation list (CRL) distribution points can be found at Specify CRL Distribution Points

Certificate Revocation Checking and CRL Distribution Points

A certificate revocation check is required for the IP-HTTPS connection between the DirectAccess client and the DirectAccess server. If the certificate revocation check fails, DirectAccess clients cannot make IP-HTTPS-based connections to a DirectAccess server. Therefore, an Internet-based CRL distribution point location must be present in the IP-HTTPS certificate and available for DirectAccess clients that are connected to the Internet.

A certification revocation check is required for the IP-HTTPS-based connection between the DirectAccess client and the network location server. If the certificate revocation check fails, DirectAccess clients cannot access an IP-HTTPS-based URL on the network location server. Therefore, an intranet-based CRL distribution point location must be present in the network location server certificate and be available for DirectAccess clients that are connected to the intranet, even when there are DirectAccess rules in the Name Resolution Policy Table (NRPT).

A certification revocation check is required for the IPsec tunnels between the DirectAccess client and the DirectAccess server.

DirectAccess clients may not be able to connect to a DirectAccess server with error 0x800b0109 when using IP-HTTPS

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where DirectAccess clients fail to connect to a server by using IP-HTTPS.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2980667

Symptoms

DirectAccess clients may not be able to connect to a DirectAccess server by using IP-HTTPS. When you run the `netsh interface http show interface` command, the output is as follows:

> URL: `https://da.contoso.com:443/IPHTTPS` Error: 0x800b0109
> Interface Status: Failed to connect to the IPHTTPS server. Waiting to reconnect
>
> The error 0x800b0109 translates to:
> CERT_E_UNTRUSTEDROOT
> # A certificate chain processed, but terminated in a root
> # certificate which is not trusted by the trust provider.

By default, the Trusted Root Certification Authorities certificate store is configured with a set of public certification authorities that are trusted by a Windows client. Some organizations may want to manage certificate trust and prevent users in the domain from configuring their own set of trusted root certificates. In addition, some organizations may want to issue certificates for the IP-HTTPS server from their own certification authority server. They need to distribute that specific trusted root certificate to enable the trust relationships. When configuring certificates for DirectAccess, the Root Certificate Authority must be trusted by the clients, and it should have the Root CA certificate in the Trusted Root Certification Authorities store.

For more information about certificates, see How certificate revocation works.

Cause

The issuing certificate authority for the IP-HTTPS certificate is not present in the clients Trusted and Intermediate stores. Make sure that you add the Root certificate to the Root store and the Intermediate certificates to the Intermediate stores.

Resolution

To solve this issue, follow these steps:

1. Obtain the certificate for the certification authority that issued the IP-HTTPS certificate.
2. Import this certificate into the computer store of the DirectAccess client.
3. To apply this change to all clients, use Group Policy to deploy the imported certificate.

DirectAccess connectivity methods

DirectAccess clients use multiple methods to connect to the DirectAccess server, which enables access to internal resources. Clients have the option to use either Teredo, 6to4, or IP-HTTPS to connect to DirectAccess. This also depends on how the DirectAccess server is configured.

When the DirectAccess client has a public IPv4 address, it will try to connect by using the 6to4 interface. However, some ISPs give the illusion of a public IP Address. What they provide to end users is a pseudo public IP address. What this means is that the IP address received by the DirectAccess client (a data card or SIM connection) might be an IP from the public address space, but in reality is behind one or more NATs.

When the client is behind a NAT device, it will try to use Teredo. Many businesses such as hotels, airports, and coffee shops do not allow Teredo traffic to traverse their firewall. In such scenarios, the client will fail over to IP-HTTPS. IP-HTTPS is built over an SSL (TLS) TCP 443-based connection. SSL outbound traffic will most likely be allowed on all networks.

Having this in mind, IP-HTTPS was built to provide a backup connection that is reliable and always reachable. A DirectAccess client will make use of this when other methods (such as Teredo or 6to4) fail.

More information about transition technologies can be found at IPv6 transition technologies.

DirectAccess clients that use Teredo tunneling cannot connect after upgrade to Windows 10

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where DirectAccess clients that use Teredo tunneling cannot connect after upgrade to Windows 10.

Applies to: Windows 10, version 1809, and later versions, Windows 10, version 1803
Original KB number: 4510763

Symptoms

On a computer on which you have DirectAccess clients configured to use Teredo tunneling, you upgrade the operating system to Windows 10, version 1803 and later versions of Windows 10. After the upgrade, the DirectAccess clients cannot connect.

At this point, if you run `netsh interface teredo`, the command returns a message that states that Teredo tunneling is disabled.

Cause

This issue occurs because Teredo tunneling is disabled by default in Windows 10, version 1803 and later versions of Windows 10.

Resolution

How to avoid this issue

Before you upgrade the system to Windows 10, make sure that Teredo tunneling is enabled by using Group Policy.

To do this, browse to the following policy in Group Policy:
Computer Configuration > **Policies** > **Administrative Templates** > **Network** > **TCPIP Settings** > **IPV6 Transition Technologies** > **Set Teredo State**

Then, set the states to **Client** or **Enterprise Client**.

How to fix this issue

If you already experience this issue, use one of the following methods to fix it.

- Run the following command on each DA client to enable Teredo tunneling:

  Console

  ```
  netsh interface teredo set state Enterprise
  ```

- Configure the **Set Teredo State** Group Policy that is mentioned under "How to avoid this issue" to enable Teredo tunneling.

> **Note**
>
> If you have to connect to the internal resource remotely to configure the policy, use IPHTTPS to connect to the DirectAccess Server or use VPN.

How to disconnect an incoming VPN connection

Article • 09/23/2021 • 2 minutes to read

This article describes how to disconnect an incoming VPN connection when an option to disconnect the incoming VPN connection is not displayed in the View Available Networks dialog box.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2737610

> ⓘ **Note**
>
> When you right-click an incoming VPN connection in Windows Server 2012 and then click **Connect/Disconnect**, the **View Available Networks** dialog box appears. However, an option to disconnect the incoming VPN connection is not displayed.

More information

To disconnect an incoming VPN connection, follow these steps:

1. Open Network Connections. To do this, use either of the following methods:
   - Swipe in from the right edge of the screen, or point to the lower-right corner of the screen, and then click **Search.** Then, type ncpa.cpl, and then click the **Ncpa.cpl** icon.
   - Press Win+R to open the **Run** window, type ncpa.cpl, and then click **OK**.
2. Right-click the incoming VPN connection that you want to disconnect, and then click **Status**.
3. On the **General** tab, click **Disconnect**.
4. Close Network Connections.

You receive an "Error 721" error message when you try to establish a VPN connection through your Windows Server-based remote access server

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an Error 721 that occurs when try to establish a VPN connection through your Windows Server-based remote access server.

Applies to: Windows 10 - all editions
Original KB number: 888201

Symptoms

If you try to establish a virtual private network (VPN) connection to a corporate network by using a Point-to-Point Tunneling Protocol (PPTP) client, the connection to the Microsoft Windows Server-based remote access server may not succeed. You may receive the following error message:

> Error 721: The remote computer is not responding.

> **Note**
>
> The 721 error description may vary.

Cause

This issue may occur if the network firewall does not permit Generic Routing Encapsulation (GRE) protocol traffic. GRE is IP Protocol 47. PPTP uses GRE for tunneled data.

Resolution

To resolve this issue, configure the network firewall to permit GRE protocol 47. Also, make sure that the network firewall permits TCP traffic on port 1723. Both of these conditions must be met to establish VPN connectivity by using PPTP.

More information

For more information about installing and configuring a VPN Server in Windows Server 2003, click the following article number to view the article in the Microsoft Knowledge Base:

323441 How to install and configure a Virtual Private Network server in Windows Server 2003

For more information about the PPTP protocol, visit the following Microsoft Web site: https://technet.microsoft.com/library/bb877963.aspx

List of error codes for dial-up connections or VPN connections

Article • 09/23/2021 • 14 minutes to read

This article lists the error codes that you may receive when you make a dial-up connection or a VPN connection.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 824864

> **Note**
>
> Error codes with numbers higher than 900 will only be seen if you are trying to connect to a Routing and Remote Access Server that is running Windows 2000 or later.

Error codes

The following list contains the error codes for dial-up connections or VPN connections:

- 600

  An operation is pending.

- 601

  The port handle is invalid.

- 602

  The port is already open.

- 603

  Caller's buffer is too small.

- 604

  Wrong information specified.

- 605

  Cannot set port information.

- 606

  The port is not connected.

- 607

  The event is invalid.

- 608

  The device does not exist.

- 609

  The device type does not exist.

- 610

  The buffer is invalid.

- 611

  The route is not available.

- 612

  The route is not allocated.

- 613

  Invalid compression specified.

- 614

  Out of buffers.

- 615

  The port was not found.

- 616

  An asynchronous request is pending.

- 617

  The port or device is already disconnecting.

- 618

The port is not open.

- 619

  The port is disconnected.

- 620

  There are no endpoints.

- 621

  Cannot open the phone book file.

- 622

  Cannot load the phone book file.

- 623

- Cannot find the phone book entry.

- 624

  Cannot write the phone book file.

- 625

  Invalid information found in the phone book.

- 626

  Cannot load a string.

- 627

  Cannot find key.

- 628

  The port was disconnected.

- 629

  The port was disconnected by the remote machine.

- 630

  The port was disconnected due to hardware failure.

- 631

  The port was disconnected by the user.

- 632

  The structure size is incorrect.

- 633

  The port is already in use or is not configured for Remote Access dialout.

- 634

  Cannot register your computer on the remote network.

- 635

  Unknown error.

- 636

  The wrong device is attached to the port.

- 637

  The string could not be converted.

- 638

  The request has timed out.

- 639

  No asynchronous net available.

- 640

  A NetBIOS error has occurred.

- 641

  The server cannot allocate NetBIOS resources needed to support the client.

- 642

  One of your NetBIOS names is already registered on the remote network.

- 643

A network adapter at the server failed.

- 644

  You will not receive network message popups.

- 645

  Internal authentication error.

- 646

  The account is not permitted to log on at this time of day.

- 647

  The account is disabled.

- 648

  The password has expired.

- 649

  The account does not have Remote Access permission.

- 650

  The Remote Access server is not responding.

- 651

  Your modem (or other connecting device) has reported an error.

- 652

  Unrecognized response from the device.

- 653

  A macro required by the device was not found in the device .INF file section.

- 654

  A command or response in the device .INF file section refers to an undefined macro

- 655

The <message> macro was not found in the device .INF file section.

- 656

  The <defaultoff> macro in the device .INF file section contains an undefined macro

- 657

  The device .INF file could not be opened.

- 658

  The device name in the device .INF or media .INI file is too long.

- 659

  The media .INI file refers to an unknown device name.

- 660

  The device .INF file contains no responses for the command.

- 661

  The device .INF file is missing a command.

- 662

  Attempted to set a macro not listed in device .INF file section.

- 663

  The media .INI file refers to an unknown device type.

- 664

  Cannot allocate memory.

- 665

  The port is not configured for Remote Access.

- 666

  Your modem (or other connecting device) is not functioning.

- 667

  Cannot read the media .INI file.

- 668

  The connection dropped.

- 669

  The usage parameter in the media .INI file is invalid.

- 670

  Cannot read the section name from the media .INI file.

- 671

  Cannot read the device type from the media .INI file.

- 672

  Cannot read the device name from the media .INI file.

- 673

  Cannot read the usage from the media .INI file.

- 674

  Cannot read the maximum connection BPS rate from the media .INI file.

- 675

  Cannot read the maximum carrier BPS rate from the media .INI file.

- 676

  The line is busy.

- 677

  A person answered instead of a modem.

- 678

  There is no answer.

- 679

  Cannot detect carrier.

- 680

There is no dial tone.

- 681

  General error reported by device.

- 682

  ERROR WRITING SECTIONNAME

- 683

  ERROR WRITING DEVICETYPE

- 684

  ERROR WRITING DEVICENAME

- 685

  ERROR WRITING MAXCONNECTBPS

- 686

  ERROR WRITING MAXCARRIERBPS

- 687

  ERROR WRITING USAGE

- 688

  ERROR WRITING DEFAULTOFF

- 689

  ERROR READING DEFAULTOFF

- 690

  ERROR EMPTY INI FILE

- 691

  Access denied because username and/or password is invalid on the domain.

- 692

  Hardware failure in port or attached device.

- 693

  ERROR NOT BINARY MACRO

- 694

  ERROR DCB NOT FOUND

- 695

  ERROR STATE MACHINES NOT STARTED

- 696

  ERROR STATE MACHINES ALREADY STARTED

- 697

  ERROR PARTIAL RESPONSE LOOPING

- 698

  A response keyname in the device .INF file is not in the expected format.

- 699

  The device response caused buffer overflow.

- 700

  The expanded command in the device .INF file is too long.

- 701

  The device moved to a BPS rate not supported by the COM driver.

- 702

  Device response received when none expected.

- 703

  ERROR INTERACTIVE MODE

- 704

  ERROR BAD CALLBACK NUMBER

- 705

ERROR INVALID AUTH STATE

- 706

  ERROR WRITING INITBPS

- 707

  X.25 diagnostic indication.

- 708

  The account has expired.

- 709

  Error changing password on domain.

- 710

  Serial overrun errors were detected while communicating with your modem.

- 711

  RasMan initialization failure. Check the event log.

- 712

  Biplex port is initializing. Wait a few seconds and redial.

- 713

  No active ISDN lines are available.

- 714

  Not enough ISDN channels are available to make the call.

- 715

  Too many errors occurred because of poor phone line quality.

- 716

  The Remote Access IP configuration is unusable.

- 717

  No IP addresses are available in the static pool of Remote Access IP addresses.

- 718

  PPP timeout.

- 719

  PPP terminated by remote machine.

- 720

  No PPP control protocols configured.

- 721

  Remote PPP peer is not responding.

- 722

  The PPP packet is invalid.

- 723

  The phone number, including prefix and suffix, is too long.

- 724

  The IPX protocol cannot dial-out on the port because the computer is an IPX router.

- 725

  The IPX protocol cannot dial-in on the port because the IPX router is not installed.

- 726

  The IPX protocol cannot be used for dial-out on more than one port at a time.

- 727

  Cannot access TCPCFG.DLL.

- 728

  Cannot find an IP adapter bound to Remote Access.

- 729

  SLIP cannot be used unless the IP protocol is installed.

- 730

  Computer registration is not complete.

- 731

  The protocol is not configured.

- 732

  The PPP negotiation is not converging.

- 733

  The PPP control protocol for this network protocol is not available on the server.

- 734

  The PPP link control protocol terminated.

- 735

  The requested address was rejected by the server.

- 736

  The remote computer terminated the control protocol.

- 737

  Loopback detected.

- 738

  The server did not assign an address.

- 739

  The remote server cannot use the Windows NT encrypted password.

- 740

  The TAPI devices configured for Remote Access failed to initialize or were not installed correctly.

- 741

  The local computer does not support encryption.

- 742

  The remote server does not support encryption.

- 743

  The remote server requires encryption.

- 744

  Cannot use the IPX net number assigned by the remote server. Check the event log.

- 745

  ERROR_INVALID_SMM

- 746

  ERROR_SMM_UNINITIALIZED

- 747

  ERROR_NO_MAC_FOR_PORT

- 748

  ERROR_SMM_TIMEOUT

- 749

  ERROR_BAD_PHONE_NUMBER

- 750

  ERROR_WRONG_MODULE

- 751

  The callback number contains an invalid character. Only the following 18 characters are allowed: 0 to 9, T, P, W, (,), -, @, and space

- 752

  A syntax error was encountered while processing a script.

- 753

The connection could not be disconnected because it was created by the multi-protocol router.

- 754

  The system could not find the multi-link bundle.

- 755

  The system cannot perform automated dial because this connection has a custom dialer specified.

- 756

  This connection is already being dialed.

- 757

  Remote Access Services could not be started automatically. Additional information is provided in the event log.

- 758

  Internet Connection Sharing is already enabled on the connection.

- 759

  An error occurred while the existing Internet Connection Sharing settings were being changed.

- 760

  An error occurred while routing capabilities were being enabled.

- 761

  An error occurred while Internet Connection Sharing was being enabled for the connection.

- 762

  An error occurred while the local network was being configured for sharing.

- 763

  Internet Connection Sharing cannot be enabled. There is more than one LAN connection other than the connection to be shared.

- 764

  No smart card reader is installed.

- 765

  Internet Connection Sharing cannot be enabled. A LAN connection is already configured with the IP address that is required for automatic IP addressing.

- 766

  A certificate could not be found. Connections that use the L2TP protocol over IPSec require the installation of a machine certificate, also known as a computer certificate.

- 767

  Internet Connection Sharing cannot be enabled. The LAN connection selected as the private network has more than one IP address configured. Reconfigure the LAN connection with a single IP address before enabling Internet Connection Sharing.

- 768

  The connection attempt failed because of failure to encrypt data.

- 769

  The specified destination is not reachable.

- 770

  The remote computer rejected the connection attempt.

- 771

  The connection attempt failed because the network is busy.

- 772

  The remote computer's network hardware is incompatible with the type of call requested.

- 773

  The connection attempt failed because the destination number has changed.

- 774

The connection attempt failed because of a temporary failure. Try connecting again.

- 775

  The call was blocked by the remote computer.

- 776

  The call could not be connected because the remote computer has invoked the Do Not Disturb feature.

- 777

  The connection attempt failed because the modem (or other connecting device on the remote computer is out of order.

- 778

  It was not possible to verify the identity of the server.

- 779

  To dial out using this connection, you must use a smart card.

- 780

  An attempted function is not valid for this connection.

- 781

  The connection requires a certificate, and no valid certificate was found. For further assistance, click More Info or search Help and Support Center for this error number.

- 782

  Internet Connection Sharing (ICS and Internet Connection Firewall (ICF cannot be enabled because Routing and Remote Access has been enabled on this computer. To enable ICS or ICF, first disable Routing and Remote Access. For more information about Routing and Remote Access, ICS, or ICF, see Help and Support.

- 783

  Internet Connection Sharing cannot be enabled. The LAN connection selected as the private network is either not present, or is disconnected from the network.

Ensure that the LAN adapter is connected before enabling Internet Connection Sharing.

- 784

  You cannot dial using this connection at logon time, because it is configured to use a user name different than the one on the smart card. If you want to use it at logon time, you must configure it to use the user name on the smart card.

- 785

  You cannot dial using this connection at logon time, because it is not configured to use a smart card. If you want to use it at logon time, you must edit the properties of this connection so that it uses a smart card.

- 786

  The L2TP connection attempt failed because there is no valid machine certificate on your computer for security authentication.

- 787

  The L2TP connection attempt failed because the security layer could not authenticate the remote computer.

- 788

  The L2TP connection attempt failed because the security layer could not negotiate compatible parameters with the remote computer.

- 789

  The L2TP connection attempt failed because the security layer encountered a processing error during initial negotiations with the remote computer.

- 790

  The L2TP connection attempt failed because certificate validation on the remote computer failed.

- 791

  The L2TP connection attempt failed because security policy for the connection was not found.

- 792

The L2TP connection attempt failed because security negotiation timed out.

- 793

  The L2TP connection attempt failed because an error occurred while negotiating security.

- 794

  The Framed Protocol RADIUS attribute for this user is not PPP.

- 795

  The Tunnel Type RADIUS attribute for this user is not correct.

- 796

  The Service Type RADIUS attribute for this user is neither Framed nor Callback Framed.

- 797

  A connection to the remote computer could not be established because the modem was not found or was busy. For further assistance, click More Info or search Help and Support Center for this error number.

- 798

  A certificate could not be found that can be used with this Extensible Authentication Protocol.

- 799

  Internet Connection Sharing (ICS cannot be enabled due to an IP address conflict on the network. ICS requires the host be configured to use 192.168.0.1. Ensure that no other client on the network is configured to use 192.168.0.1.

- 800

  Unable to establish the VPN connection. The VPN server may be unreachable, or security parameters may not be configured properly for this connection.

- 801

  This connection is configured to validate the identity of the access server, but Windows cannot verify the digital certificate sent by the server.

- 802

The card supplied was not recognized. Check that the card is inserted correctly, and fits tightly.

- 803

  The PEAP configuration stored in the session cookie does not match the current session configuration.

- 804

  The PEAP identity stored in the session cookie does not match the current identity.

- 805

  You cannot dial using this connection at logon time, because it is configured to use logged on user's credentials.

- 900

  The router is not running.

- 901

  The interface is already connected.

- 902

  The specified protocol identifier is not known to the router.

- 903

  The Demand-dial Interface Manager is not running.

- 904

  An interface with this name is already registered with the router.

- 905

  An interface with this name is not registered with the router.

- 906

  The interface is not connected.

- 907

  The specified protocol is stopping.

- 908

  The interface is connected and hence cannot be deleted.

- 909

  The interface credentials have not been set.

- 910

  This interface is already in the process of connecting.

- 911

  An update of routing information on this interface is already in progress.

- 912

  The interface configuration in invalid. There is already another interface that is connected to the same interface on the remote router.

- 913

  A Remote Access Client attempted to connect over a port that was reserved for Routers only.

- 914

  A Demand Dial Router attempted to connect over a port that was reserved for Remote Access Clients only.

- 915

  The client interface with this name already exists and is currently connected.

- 916

  The interface is in a disabled state.

- 917

  The authentication protocol was rejected by the remote peer.

- 918

  There are no authentication protocols available for use.

- 919

The remote computer refused to be authenticated using the configured authentication protocol. The line has been disconnected.

- 920

  The remote account does not have Remote Access permission.

- 921

  The remote account has expired.

- 922

  The remote account is disabled.

- 923

  The remote account is not permitted to logon at this time of day.

- 924

  Access was denied to the remote peer because username and/or password is invalid on the domain.

- 925

  There are no routing enabled ports available for use by this demand dial interface.

- 926

  The port has been disconnected due to inactivity.

- 927

  The interface is not reachable at this time.

- 928

  The Demand Dial service is in a paused state.

- 929

  The interface has been disconnected by the administrator.

- 930

  The authentication server did not respond to authentication requests in a timely fashion.

- 931

  The maximum number of ports allowed for use in the multilinked connection has been reached.

- 932

  The connection time limit for the user has been reached.

- 933

  The maximum limit on the number of LAN interfaces supported has been reached.

- 934

  The maximum limit on the number of Demand Dial interfaces supported has been reached.

- 935

  The maximum limit on the number of Remote Access clients supported has been reached.

- 936

  The port has been disconnected due to the BAP policy.

- 937

  Because another connection of your type is in use, the incoming connection cannot accept your connection request.

- 938

  No RADIUS servers were located on the network.

- 939

  An invalid response was received from the RADIUS authentication server. Make sure that the case-sensitive secret password for the RADIUS server is set correctly.

- 940

  You do not have permission to connect at this time.

- 941

  You do not have permission to connect using the current device type.

- 942

  You do not have permission to connect using the selected authentication protocol.

- 943

  BAP is required for this user.

- 944

  The interface is not allowed to connect at this time.

- 945

  The saved router configuration is incompatible with the current router.

- 946

  RemoteAccess has detected older format user accounts that will not be migrated automatically. To migrate these manually, run XXXX.

- 948

  The transport is already installed with the router.

- 949

  Received invalid signature length in packet from RADIUS server.

- 950

  Received invalid signature in packet from RADIUS server.

- 951

  Did not receive signature along with EAPMessage from RADIUS server.

- 952

  Received packet with invalid length or Id from RADIUS server.

- 953

  Received packet with attribute with invalid length from RADIUS server.

- 954

  Received invalid packet from RADIUS server.

- 955

  Authenticator does not match in packet from RADIUS server.

Modern Apps can't connect when you use a Check Point VPN connection

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where Modern Apps can't connect to the Internet after you connect to the corporate network by using Check Point VPN software.

Applies to: Windows 8
Original KB number: 2855849

Symptoms

Consider the following scenario:

- You use a version of Check Point Endpoint Remote Access VPN that is earlier than E80.50.
- You're running Windows 8 Modern Applications (Store Apps) and classic desktop applications successfully.
- You connect to the corporate network by having the Check Point VPN client software in "hub mode" (that is, all traffic is routed through the virtual network adapter).
- After you make the connection, the Network Status indicator shows that Internet connectivity is fully available.

In this scenario, Classic Apps can connect successfully to the Internet. However, Modern Apps can't connect. Also, the desktop version of Windows Internet Explorer 10 can't connect if Enhanced Security Mode is enabled.

Cause

This issue occurs because the installed firewall can't set rules that allow Modern Apps to communicate through the virtual private network.

Resolution

To resolve this issue, install Check Point VPN E80.50 (expected to be available Fall 2013) from the following Check Point Support Center website:

Remote Access (VPN) Clients

Workaround

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

To work around this issue, run following Windows PowerShell script to change the hidden property for the virtual network interface in the registry:

PowerShell

```
foreach ($subkey in (gci "HKLM:\SYSTEM\CurrentControlSet\Control\Class\
{4D36E972-E325-11CE-BFC1-08002bE10318} -erroraction silentlycontinue))
{
    if ((get-itemproperty $subkey.pspath).ComponentID eq cp_apvna)
    {
        set-itemproperty $subkey.pspath name Characteristics value 0x1
    }
}
```

> **Note**
>
> This script is also documented at the following Check Point website: **Microsoft Store (Windows 8) application fails to communicate via VPN tunnel**

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft doesn't guarantee the accuracy of this third-party contact information.

How to troubleshoot a Microsoft L2TP/IPSec virtual private network client connection

Article • 09/23/2021 • 3 minutes to read

This article describes how to troubleshoot L2TP/IPSec virtual private network (VPN) connection issues.

Applies to: Windows 10 - all editions
Original KB number: 325034

Summary

You must have an Internet connection before you can make an L2TP/IPSec VPN connection. If you try to make a VPN connection before you have an Internet connection, you may experience a long delay, typically 60 seconds, and then you may receive an error message that says there was no response or something is wrong with the modem or other communication device.

When you troubleshoot L2TP/IPSec connections, it's useful to understand how an L2TP/IPSec connection proceeds. When you start the connection, an initial L2TP packet is sent to the server, requesting a connection. This packet causes the IPSec layer on your computer to negotiate with the VPN server to set up an IPSec protected session (a security association). Depending on many factors including link speed, the IPSec negotiations may take from a few seconds to around two minutes. When an IPSec security association (SA) has been established, the L2TP session starts. When it starts, you receive a prompt for your name and password (unless the connection has been set up to connect automatically in Windows Millennium Edition.) If the VPN server accepts your name and password, the session setup completes.

A common configuration failure in an L2TP/IPSec connection is a misconfigured or missing certificate, or a misconfigured or missing preshared key. If the IPSec layer can't establish an encrypted session with the VPN server, it will fail silently. As a result, the L2TP layer doesn't see a response to its connection request. There will be a long delay, typically 60 seconds, and then you may receive an error message that says there was no response from the server or there was no response from the modem or communication device. If you receive this error message before you receive the prompt for your name and password, IPSec didn't establish its session. If that occurs, examine your certificate or preshared key configuration, or send the isakmp log to your network administrator.

A second common problem that prevents a successful IPSec session is using a Network Address Translation (NAT). Many small networks use a router with NAT functionality to share a single Internet address among all the computers on the network. The original version of IPSec drops a connection that goes through a NAT because it detects the NAT's address-mapping as packet tampering. Home networks frequently use a NAT. This blocks using L2TP/IPSec unless the client and the VPN gateway both support the emerging IPSec NAT-Traversal (NAT-T) standard. For more information, see the "NAT Traversal" section.

If the connection fails after you receive the prompt for your name and password, the IPSec session has been established and there's probably something wrong with your name and password. Other server settings may also be preventing a successful L2TP connection. In this case, send the PPP log to your administrator.

NAT Traversal

With the IPSec NAT-T support in the Microsoft L2TP/IPSec VPN client, IPSec sessions can go through a NAT when the VPN server also supports IPSec NAT-T. IPSec NAT-T is supported by Windows Server 2003. IPSec NAT-T is also supported by Windows 2000 Server with the L2TP/IPSec NAT-T update for Windows XP and Windows 2000.

For third-party VPN servers and gateways, contact your administrator or VPN gateway vendor to verify that IPSec NAT-T is supported.

More information

The configuration utility also provides a check box that enables IPSec logging. If you can't connect, and your network administrator or support personnel have asked you to provide them a connection log, you can enable IPSec logging here. When you do so, the log (Isakmp.log) is created in the `C:\Program Files\Microsoft IPSec VPN` folder. When you create a connection, also enable logging for the PPP processing in L2TP. To do so:

1. Right-click the **Dialup Networking** folder, and then click **Properties**.
2. Click the **Networking** tab, and then click to select the **Record a log file for this connection** check box.

The PPP log file is `C:\Windows\Ppplog.txt`. It's located in the `C:\Program Files\Microsoft IPSec VPN` folder.

For more information, see Default Encryption Settings for the Microsoft L2TP/IPSec Virtual Private Network Client.

Windows Connection Manager disconnects WLAN if a VPN connection is established

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution for the issue that Windows Connection Manager disconnects WLAN if a VPN connection is established.

Applies to: Windows 8 Pro
Original KB number: 2919900

Symptom

Consider the following scenario:

- You start a Windows 8 client. It connects automatically to a WLAN.
- You establish a Virtual Private Network (VPN) connection on the Windows 8 client.
- About 20 seconds after the VPN tunnel is established successfully, the WLAN connection is disconnected.

Cause

This issue occurs because the VPN Adapter is registered as an Ethernet adapter.

To check this, open registry editor, and then browse to this key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}\xxxx`

`"*IfType"=dword:00000006 ==> IF_TYPE_ETHERNET_CSMACD`

> **Note**
>
> xxxx corresponds to the number below that you can find the name of your VPN Adapter. If the value for IfType equals to 6, the Adapter is considered an Ethernet Adapter.

Starting with Windows 8, the WCMSVC (Windows Connection Manager) disconnects the WLAN connection because an Ethernet Adapter is seen as more reliable and provides

better performance compared to a WLAN connection. These items are taken into account during the decision:

- Adapter type, Ethernet, wireless, virtual
- Does an adapter hold the default gateway and default route?
- Does Network Connectivity Status Indicator (NCSI) probe that the adapter is successfully connected to the Internet?
- Is the client's domain reachable on the adapter?

Resolution

Configure the Windows Connection Manager GPO to "Disabled" by using Group Policy or locally.

1. Open Local Group Policy Editor, and then go to Computer Configuration\Administrative Templates\Network\Windows Connection Manager
2. Change the Setting of **Minimize the number of simultaneous connections to the Internet or a Windows Domain** to "disabled"

More information

Alternatively you could change the IfType of the VPN interface to a value different from Ethernet.

> **Note**
>
> Changing this setting may have some side effects on the functionality of the VPN Adapter. Contact the manufacturer of the VPN Client to get more information.

The values for different Adapter types can be found here:
https://msdn.microsoft.com/library/aa814491(VS.85).aspx
https://msdn.microsoft.com/library/windows/hardware/ff565767(v=vs.85).aspx

Suitable values for VPN adapters are:

`IF_TYPE_PROP_VIRTUAL 53 (0x35) Proprietary virtual/internal`

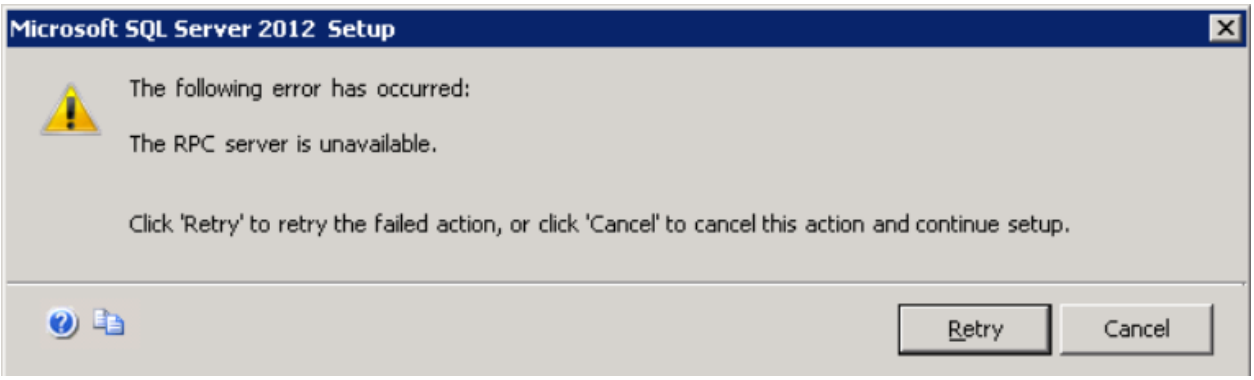
`IF_TYPE_TUNNEL 131 (0x83) Encapsulation interface`

Remote Procedure Call (RPC) errors troubleshooting guidance

Article • 12/30/2022 • 10 minutes to read

Applies to: Windows Client

You might encounter an "RPC server unavailable" error when you connect to Windows Management Instrumentation (WMI) or Microsoft SQL Server, during a Remote Procedure Call (RPC) session, or when you use various Microsoft Management Console (MMC) snap-ins. The following image shows an example of an RPC error.



This is a common networking error that requires some basic familiarity with the process to successfully troubleshoot. To begin, there are several important terms to understand:

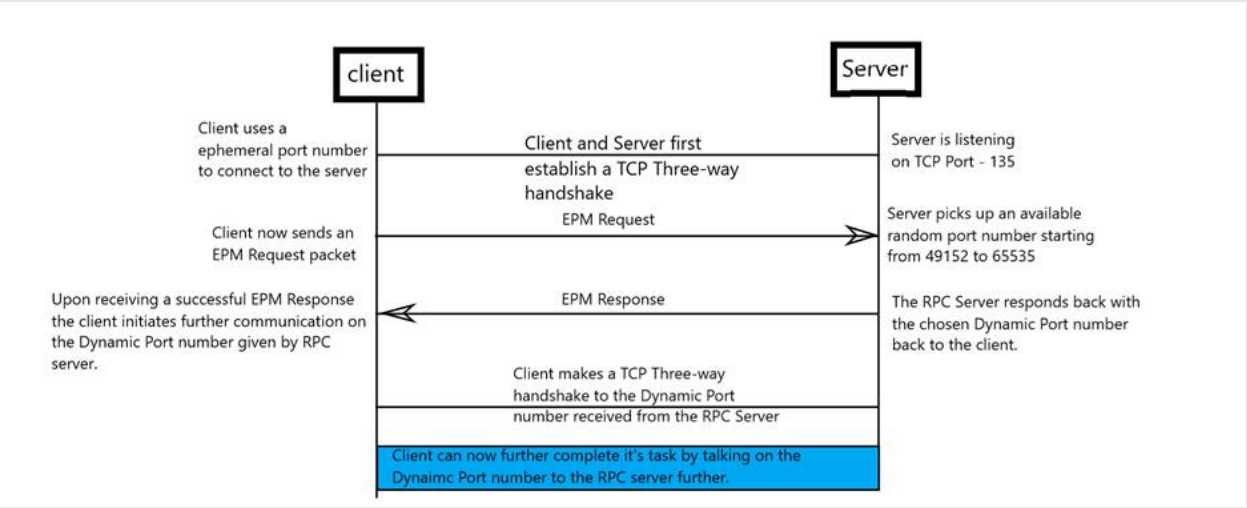
- **Endpoint mapper (EPM)**: A service that listens on the server and guides client apps to server apps by using port and UUID information.
- **Tower**: Describes the RPC protocol to enable the client and server to negotiate a connection.
- **Floors**: The layers of contents within a tower that contain specific data, such as ports, IP addresses, and identifiers.
- **UUID**: A well-known GUID that identifies an RPC application. During troubleshooting, you can use the UUID to track the RPC conversations of a single type of application (among the many types that occur on a single computer at one time).
- **Opnum**: Identifies a function that the client wants the server to perform. This is simply a hexadecimal number. However, a good network analyzer will translate the function for you. If the function can't be identified, contact your application vendor.
- **Port**: The communication endpoint for client or server application. The EPM allocates dynamic ports (also known as high ports or ephemeral ports) for clients and servers to use.

> **Note**
>
> Typically the port number is the most important information that you'll use for troubleshooting.

- **Stub data**: The data exchanged between the functions on the client and the functions on the server. This data is the payload, the important part of the communication.

How the connection works

The following diagram shows a client connecting to a server to run a remote operation. The client initially contacts TCP port 135 on the server, and then negotiates with EPM for a dynamic port number. After EPM assigns a port, the client disconnects, and then uses the dynamic port to connect to the server.



> **Important**
>
> If a firewall separates the client and the server, the firewall has to allow communication on port 135 and on the dynamic ports that EPM assigns. One approach to managing this scenario is to specify ports or ranges of ports for EPM to use. For more information, see **Configure how RPC allocates dynamic ports**.
>
> Some firewalls also allow UUID filtering. In this scenario, if an RPC request uses port 135 to cross the firewall and contact EPM, the firewall notes the UUID that's associated with the request. When EPM responds and sends a dynamic port number for that UUID, the firewall also notes the port number. The firewall then allows RPC bind operations for that UUID and port.

Configure how RPC allocates dynamic ports

By default, EPM allocates dynamic ports randomly from the range that's configured for TCP and UDP (based on the implementation of the operating system that's used). However, this approach might not be practical, especially if the client and server must communicate through a firewall. An alternative method is to specify a port number or range of port numbers for EPM to use, and open those ports in the firewall.

Many Windows server applications that rely on RPC provide options (such as registry keys) to customize the allowed ports. Windows services use the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\Internet** subkey for this task.

When you specify a port or port range, use ports that are outside the range of commonly used ports. You can find a comprehensive list of server ports that are used in Windows and major Microsoft products in Service overview and network port requirements for Windows. The article also lists RPC server applications, and mentions which RPC server applications can be configured to use custom server ports beyond the capabilities of the RPC runtime.

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For protection, back up the registry before you modify it so that you can restore it if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

By default, the **Internet** key doesn't exist. Therefore, you have to create it. For the **Internet** key, you can configure the following entries:

- **Ports REG_MULTI_SZ**: Specifies a port or inclusive range of ports. The other entries that appear under **Internet** indicate whether these are the ports to use or the ports to exclude from use.
  - Value range: **0** - **65535**
    For example, **5984** represents a single port, and **5000–5100** represents a set of ports. If any values are outside the range of **0** to **65535**, or if any value can't be interpreted, the RPC runtime treats the entire configuration as invalid.

- **PortsInternetAvailable REG_SZ**: Specifies whether the **Ports** value represents ports to include or ports to exclude.
  - Values: **Y** or **N** (not case-sensitive)

    - **Y**: The ports that are listed in the **Ports** entry represent all the ports on that computer that are available to EPM.
    - **N**: The ports that are listed in the **Ports** entry represent all ports that aren't available to EPM.

- **UseInternetPorts REG_SZ**: Specifies the default system policy.
    - Values: **Y** or **N** (not case-sensitive)
        - **Y**: The processes that use the default system policy are assigned ports from the set of internet-available ports, as defined previously.
        - **N**: The processes that use the default system policy are assigned ports from the set of intranet-only ports.

You should open a range of ports that are greater than port 5000. Port numbers that are less than 5000 might already be in use by other applications, and they could cause conflicts with your DCOM applications. Furthermore, previous experience shows that a minimum of 100 ports should be opened. This is because several system services rely on these RPC ports to communicate with one another.

> ⓘ **Note**
>
> The minimum number of ports that are required may differ from computer to computer. Computers that support more traffic might encounter port exhaustion if the RPC dynamic ports are restricted. Take this into consideration if you restrict the port range.

> ⚠ **Warning**
>
> If there's an error in the port configuration, or there aren't enough ports in the pool, EPM can't register RPC server applications (including Windows services such as Netlogon) that use dynamic endpoints. If a configuration error occurs, the error code is **87 (0x57) ERROR_INVALID_PARAMETER**. For example, if there aren't enough ports, Netlogon logs event 5820:
>
> Log Name: System
> Source: NETLOGON
> Event ID: 5820
> Level: Error
> Keywords: Classic
> Description:
> The Netlogon service could not add the AuthZ RPC interface. The service was terminated. The following error occurred: 'The parameter is incorrect.'

For more information about how RPC works, see RPC over IT/Pro.

Example of a custom port configuration

In this example, ports 5000 through 6000 (inclusive) were arbitrarily selected to help illustrate how the new registry entries can be configured. This example isn't a recommendation of a minimum number of ports that any particular system requires. Such a configuration requires adding the **Internet** key under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc**, and adding the following entries:

- **Ports MULTI_SZ**
  - Data type: **MULTI_SZ**
  - Value: **5000-6000**
- **PortsInternetAvailable REG_SZ**
  - Data type: **REG_SZ**
  - Value: **Y**
- **UseInternetPorts REG_SZ**
  - Data type: **REG_SZ**
  - Value: **Y**

The computer has to restart for this configuration to take effect. After that, all applications that use RPC are assigned dynamic ports in the range of 5000 through 6000 (inclusive).

Troubleshooting RPC errors

PortQry

PortQry provides quick insight into how RPC is functioning before you delve into network trace data. You can quickly determine whether you can make a connection by running the following command on the client computer:

```
Console

Portqry.exe -n <ServerIP> -e 135
```

> **Note**
>
> In this command, <*ServerIP*> represents the IP address of the server that you're contacting.

For example, consider the following command:

Console

```
Portqry.exe -n 169.254.0.2 -e 135
```

This command produces output that resembles the following excerpt:

Output

```
Querying target system called:
169.254.0.2
Attempting to resolve IP address to a name...
IP address resolved to RPCServer.contoso.com
querying...
TCP port 135 (epmap service): LISTENING
Using ephemeral source port
Querying Endpoint Mapper Database...
Server's response:
UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d
ncacn_ip_tcp:169.254.0.2[49664]
```

By examining this output, you can determine the following information:

- DNS is working correctly (it resolved the IP address to a fully qualified domain name (FQDN)).
- PortQry contacted the RPC port (135) on the target computer.
- EPM responded to PortQry, and assigned the dynamic port 49664 (enclosed in square brackets) for subsequent communication.
- PortQry reconnected to port 49664.

If any of these steps fail, you can usually start collecting simultaneous network traces, as described in the next section.

For more information about PortQry, see Using the PortQry command-line tool.

Netsh

You can use the Windows netsh tool to collect network trace data simultaneously on the client and the server.

To collect simultaneous network traces, open an elevated Command Prompt window on both the client and the server.

On the client, run the following command:

Console

```
Netsh trace start scenario=netconnection capture=yes
tracefile=c:\client_nettrace.etl maxsize=512 overwrite=yes report=yes
```

On the server, run the following command:

Console

```
Netsh trace start scenario=netconnection capture=yes
tracefile=c:\server_nettrace.etl maxsize=512 overwrite=yes report=yes
```

Now, try to reproduce your issue on the client computer. Then, run the following command at the command prompt in both windows to stop the traces:

Console

```
Netsh trace stop
```

Open the trace files in Microsoft Network Monitor 3.4 or Message Analyzer, and filter the trace data for the IP address of the server or client computers and TCP port 135. For example, use filter strings such as the following:

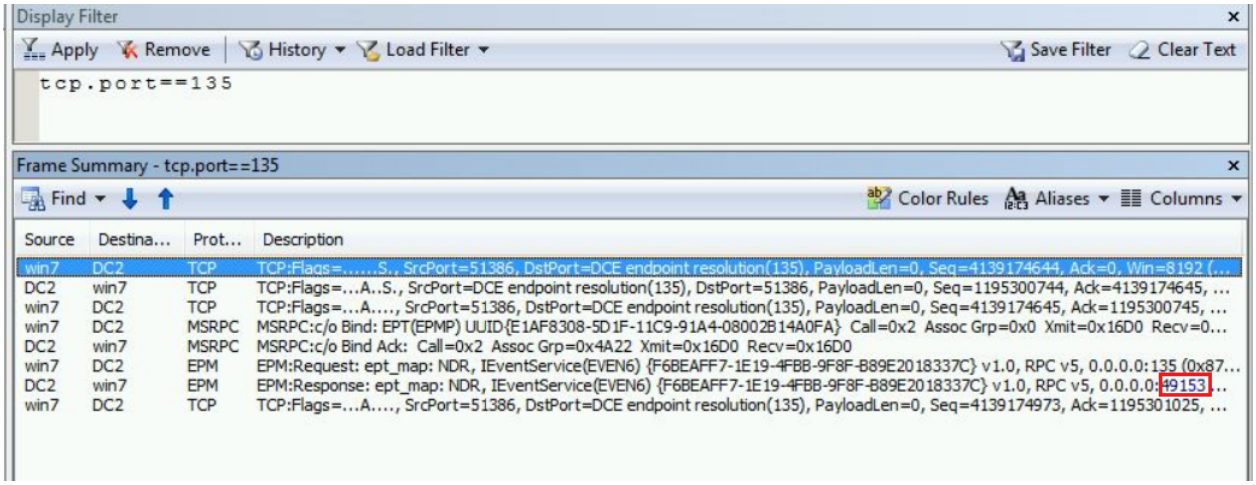
- **Ipv4.address==<*client-ip*> and ipv4.address==<*server-ip*> and tcp.port==135**

  In this filter string, <*client-ip*> represents the IP address of the client, and <*server-ip*> represents the IP address of the server.

- **tcp.port==135**

In the filtered data, look for the **EPM** entry in the **Protocol** column.

Look for a response from EPM (on the server) that includes a dynamic port number. If the dynamic port number is present, note it for future reference.



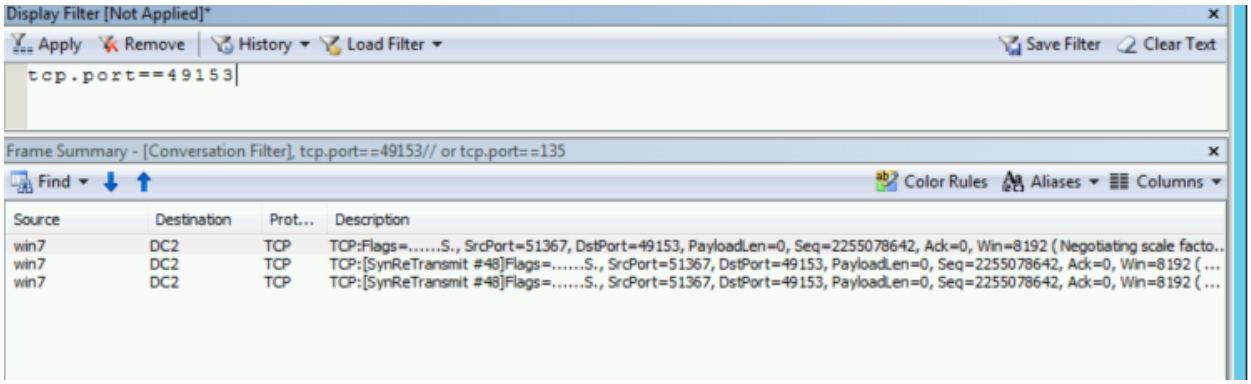
Refilter the trace data for the dynamic port number and the server IP address. For example, use a filter string such as **tcp.port==<*dynamic-port-allocated*> and ipv4.address==<*server-ip*>**. In this filter string, <*dynamic-port-allocated*> represents the dynamic port number and <*server-ip*> represents the IP address of the server.



In the filtered data, look for evidence that the client connected successfully to the dynamic port, or look for any network issues that might have occurred.

Port not reachable

The most common cause of "RPC server unavailable" errors is that the client can't connect to the dynamic port that was allocated. The client-side trace would then show TCP SYN retransmits for the dynamic port.



This behavior indicates that one of the following conditions is blocking communication:

- The dynamic port range is blocked on the firewall in the environment.
- A middle device is dropping the packets.
- The destination server is dropping the packets. This condition could be caused by such configurations as Windows Filtering Platform (WFP) packet drop, Network Interface Card (NIC) packet drop, or filter driver modifications.

Collecting data for deeper troubleshooting

Before you contact Microsoft support, we recommend that you gather information about your issue.

Prerequisites

These procedures use the TroubleShootingScript Version 2 (TSSv2) toolset. To use this toolset, you should be aware of the following prerequisites:

- You must have Administrator-level permission on the local computer.
- The first time that you run the toolset, you have to accept a EULA.
- Make sure that the Windows PowerShell script execution policy for the computer is set to `RemoteSigned`. For more information about PowerShell execution policy, see about_Execution_Policies.

  > **Note**
  >
  > If your environment prevents you from using `RemoteSigned` at the computer level, you can temporarily set it at the process level. To do this, run the following cmdlet in an elevated Powershell Command Prompt window before you start the tool:
  >
  > PowerShell
  >
  > ```
  > PS C:\> Set-ExecutionPolicy -scope Process -ExecutionPolicy
  > RemoteSigned
  > ```
  >
  > To verify that the change takes effect, run the `PS C:\> Get-ExecutionPolicy -List` cmdlet.
  >
  > The process-level permissions apply to only the current PowerShell session. After you close the PowerShell window, the execution policy reverts to the original setting.

Gather key information before contacting Microsoft support

1. Download TSSv2 on all nodes, and expand it to the *C:\tss_tool* folder.
2. Open the *C:\tss_tool* folder in an elevated PowerShell Command Prompt window.

3. Start traces on the problem computer by running the following cmdlet:

```
PowerShell

TSSv2.ps1 -Start -Scenario NET_RPC
```

4. Respond to the EULA prompt.
5. Reproduce the issue. You can use tools such as Event Viewer or wbemtest to monitor or test the issue.
6. After you reproduce the issue, immediately stop collecting data.
7. After the automated scripts finish collecting the required data, attach the data to your support request.

Troubleshoot port exhaustion issues

Article • 09/02/2022 • 9 minutes to read

Applies to: Windows 10

TCP and UDP protocols work based on port numbers used for establishing connection. Any application or a service that needs to establish a TCP/UDP connection will require a port on its side.

There are two types of ports:

- Ephemeral ports, which are dynamic ports, are the set of ports that every machine by default will have them to make an outbound connection.
- Well-known ports are the defined port for a particular application or service. For example, file server service is on port 445, HTTPS is 443, HTTP is 80, and RPC is 135. Custom application will also have their defined port numbers.

When a connection is being established with an application or service, client devices use an ephemeral port from the device to connect to a well-known port defined for that application or service. A browser on a client machine will use an ephemeral port to connect to `https://www.microsoft.com` on port 443.

In a scenario where the same browser is creating many connections to multiple websites, for any new connection that the browser is attempting, an ephemeral port is used. After some time, you'll notice that the connections will start to fail and one high possibility for this failure would be because the browser has used all the available ports to make connections outside and any new attempt to establish a connection will fail as there are no more ports available. When all the ports on a machine are used, we term it as port exhaustion.

Default dynamic port range for TCP/IP

To comply with Internet Assigned Numbers Authority (IANA) recommendations, Microsoft has increased the dynamic client port range for outgoing connections. The new default start port is 49152, and the new default end port is 65535. This increase is a change from the configuration of earlier versions of Windows that used a default port range of 1025 through 5000.

You can view the dynamic port range on a computer by using the following `netsh` commands:

- Console

```
netsh int ipv4 show dynamicport tcp
```

- Console

```
netsh int ipv4 show dynamicport udp
```

- Console

```
netsh int ipv6 show dynamicport tcp
```

- Console

```
netsh int ipv6 show dynamicport udp
```

The range is set separately for each transport (TCP or UDP). The port range is now a range that has a starting point and an ending point. Microsoft customers who deploy servers that are running Windows Server may have problems that affect RPC communication between servers if firewalls are used on the internal network. In these situations, we recommend that you reconfigure the firewalls to allow traffic between servers in the dynamic port range of 49152 through 65535. This range is in addition to well-known ports that are used by services and applications. Or, the port range that is used by the servers can be modified on each server. You adjust this range by using the netsh command, as follows. The above command sets the dynamic port range for TCP.

Console

```
netsh int <ipv4|ipv6> set dynamic <tcp|udp> start=number num=range
```

The start port is number, and the total number of ports is range. The following are sample commands:

- Console

```
netsh int ipv4 set dynamicport tcp start=10000 num=1000
```

- Console

```
netsh int ipv4 set dynamicport udp start=10000 num=1000
```

- Console

```
netsh int ipv6 set dynamicport tcp start=10000 num=1000
```

- Console

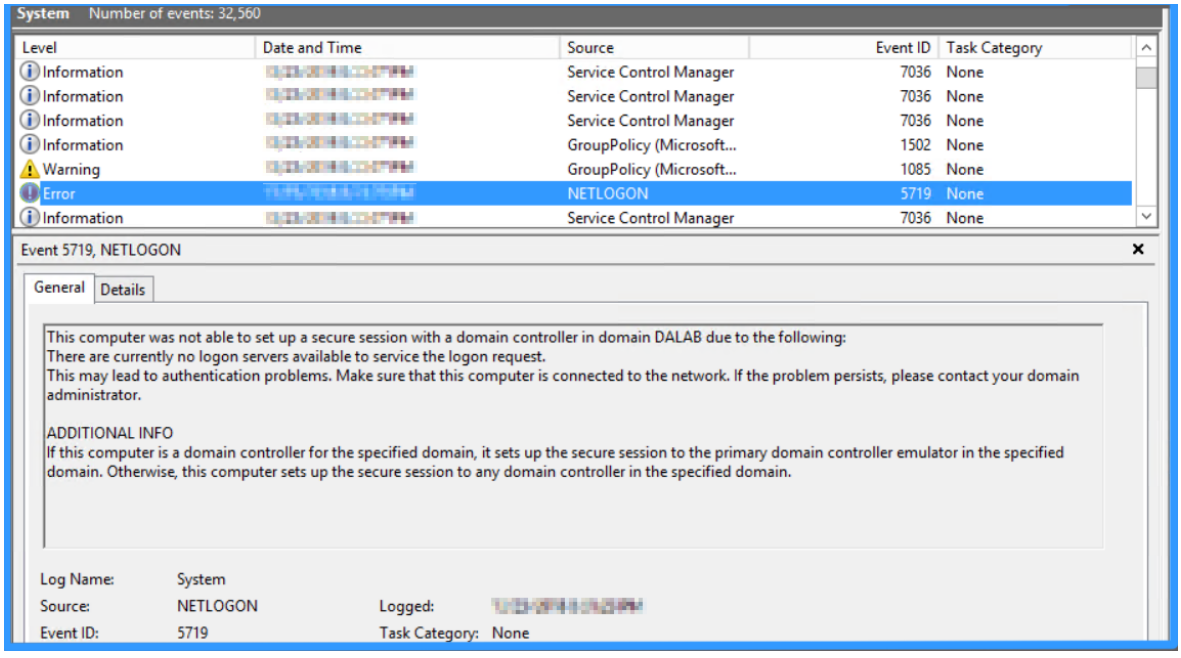
```
netsh int ipv6 set dynamicport udp start=10000 num=1000
```

These sample commands set the dynamic port range to start at port 10000 and to end at port 10999 (1000 ports). The minimum range of ports that can be set is 255. The minimum start port that can be set is 1025. The maximum end port (based on the range being configured) can't exceed 65535. To duplicate the default behavior of Windows Server 2003, use 1025 as the start port, and then use 3976 as the range for both TCP and UDP. This usage pattern results in a start port of 1025 and an end port of 5000.

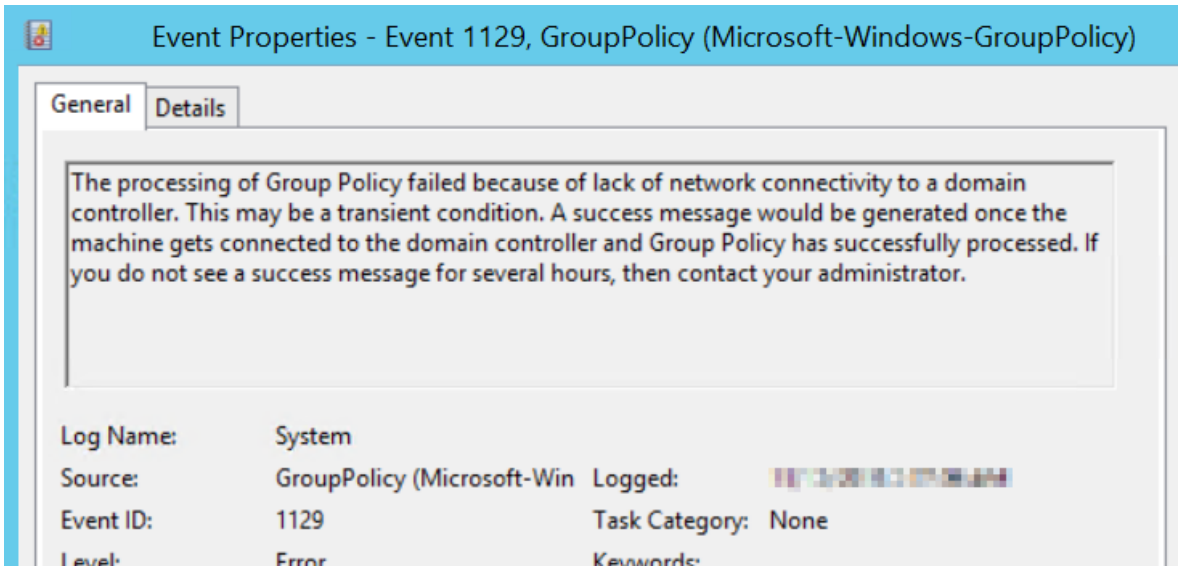
Specifically, about outbound connections as incoming connections won't require an Ephemeral port for accepting connections.

Since outbound connections start to fail, you'll see many instances of the below behaviors:

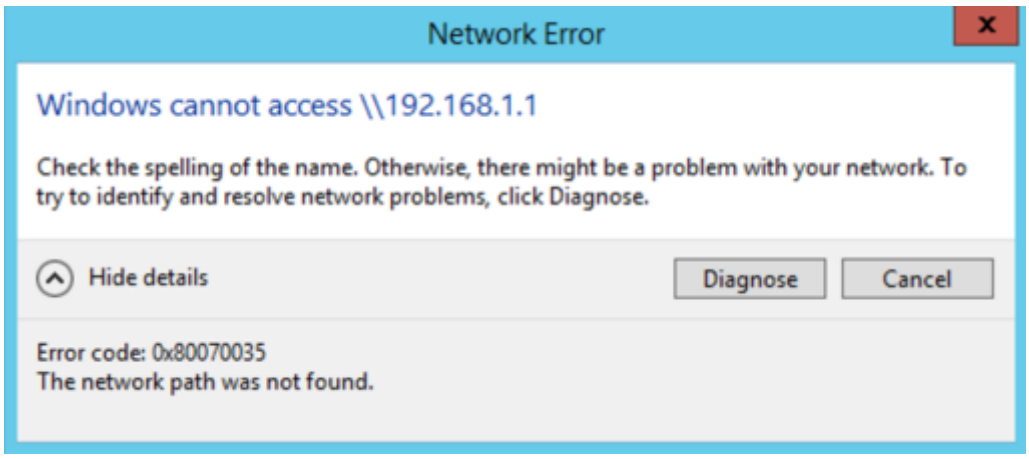
- Unable to sign in to the machine with domain credentials, however sign-in with local account works. Domain sign in will require you to contact the DC for authentication, which is again an outbound connection. If you've cache credentials set, then domain sign-in might still work.



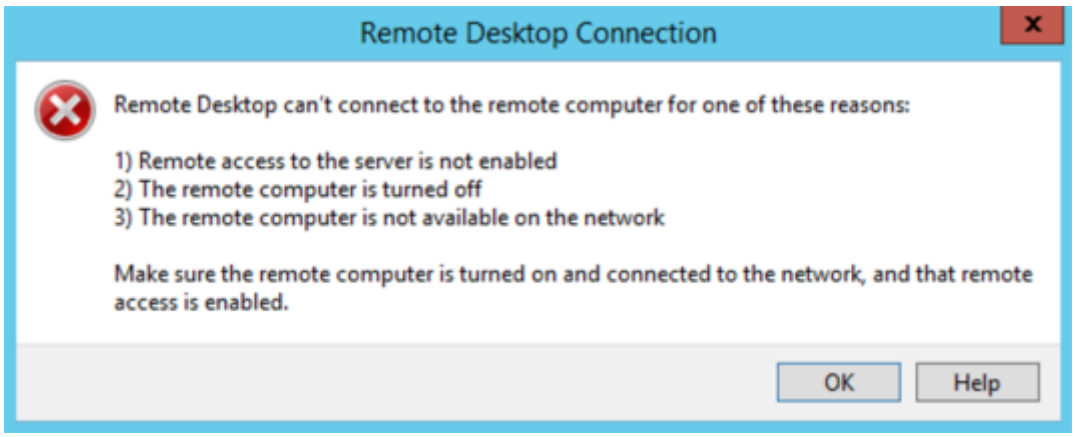
- Group Policy update failures:



- File shares are inaccessible:



- RDP from the affected server fails:



- Any other application running on the machine will start to give out errors

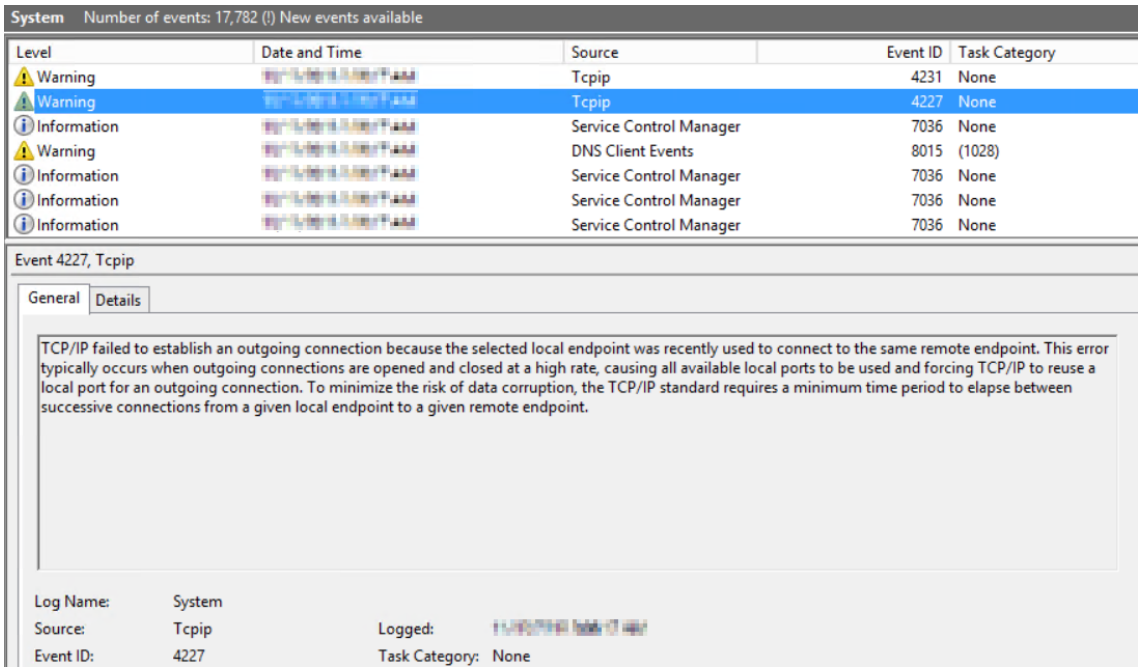
Reboot of the server will resolve the issue temporarily, but you would see all the symptoms come back after a period of time.

If you suspect that the machine is in a state of port exhaustion:

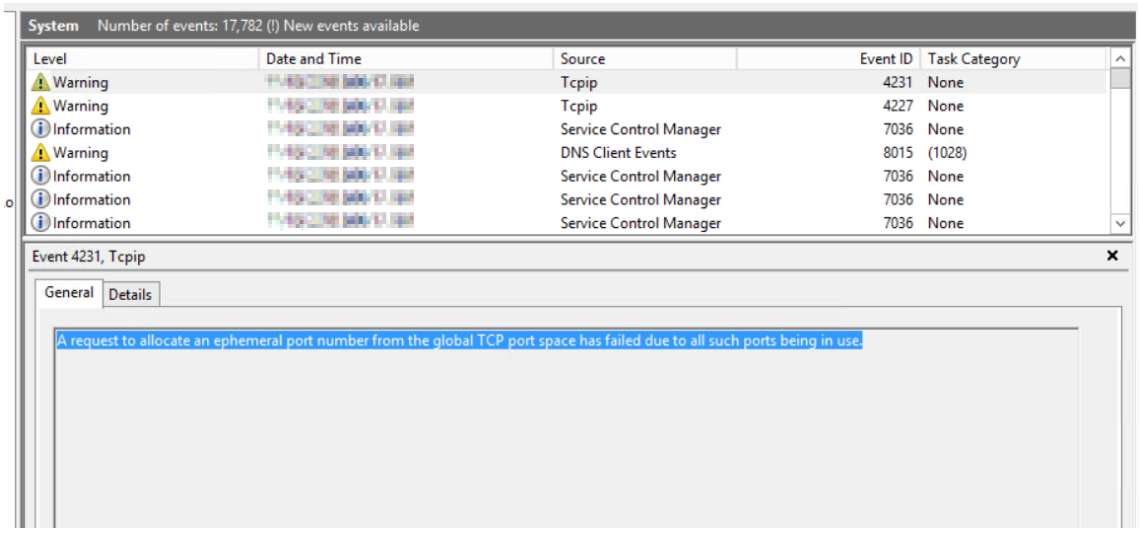
1. Try making an outbound connection. From the server/machine, access a remote share or try an RDP to another server or telnet to a server on a port. If the outbound connection fails for all of these options, go to the next step.

2. Open event viewer and under the system logs, look for the events that clearly indicate the current state:

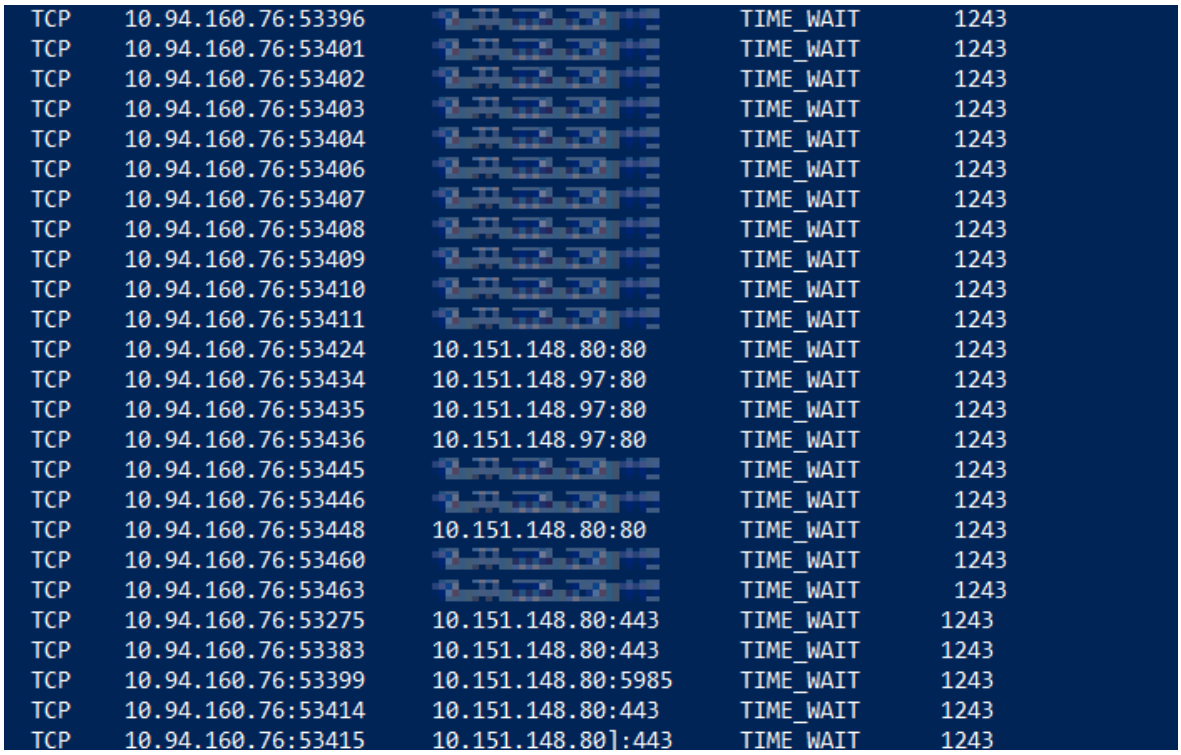
   a. Event ID 4227



   b. Event ID 4231



3. Collect a `netstat -anob` output from the server. The netstat output will show you a huge number of entries for TIME_WAIT state for a single PID.



TCP	10.94.160.76:53396	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53401	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53402	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53403	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53404	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53406	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53407	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53408	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53409	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53410	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53411	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53424	10.151.148.80:80	TIME_WAIT	1243
TCP	10.94.160.76:53434	10.151.148.97:80	TIME_WAIT	1243
TCP	10.94.160.76:53435	10.151.148.97:80	TIME_WAIT	1243
TCP	10.94.160.76:53436	10.151.148.97:80	TIME_WAIT	1243
TCP	10.94.160.76:53445	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53446	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53448	10.151.148.80:80	TIME_WAIT	1243
TCP	10.94.160.76:53460	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53463	[redacted]	TIME_WAIT	1243
TCP	10.94.160.76:53275	10.151.148.80:443	TIME_WAIT	1243
TCP	10.94.160.76:53383	10.151.148.80:443	TIME_WAIT	1243
TCP	10.94.160.76:53399	10.151.148.80:5985	TIME_WAIT	1243
TCP	10.94.160.76:53414	10.151.148.80:443	TIME_WAIT	1243
TCP	10.94.160.76:53415	10.151.148.80]:443	TIME_WAIT	1243

After a graceful closure or an abrupt closure of a session, after a period of 4 minutes (default), the port used by the process or application would be released back to the available pool. During this 4 minutes, the TCP connection state will be TIME_WAIT state. In a situation where you suspect port exhaustion, an application or process won't be able to release all the ports that it has consumed and will remain in the TIME_WAIT state.

You might also see CLOSE_WAIT state connections in the same output; however, CLOSE_WAIT state is a state when one side of the TCP peer has no more data to send (FIN sent) but is able to receive data from the other end. This state doesn't necessarily indicate port exhaustion.

> ⓘ **Note**
>
> Having huge connections in TIME_WAIT state doesn't always indicate that the server is currently out of ports unless the first two points are verified. Having lot of TIME_WAIT connections does indicate that the process is creating lot of TCP connections and may eventually lead to port exhaustion.
>
> Netstat has been updated in Windows 10 with the addition of the `-Q` switch to show ports that have transitioned out of time wait as in the BOUND state. An update for Windows 8.1 and Windows Server 2012 R2 has been released that contains this functionality. The PowerShell cmdlet `Get-NetTCPConnection` in Windows 10 also shows these BOUND ports.

> Until 10/2016, netstat was inaccurate. Fixes for netstat, back-ported to 2012 R2, allowed *Netstat.exe* and `Get-NetTcpConnection` to correctly report TCP or UDP port usage in Windows Server 2012 R2. See **Windows Server 2012 R2: Ephemeral ports hotfixes** to learn more.

4. Open a command prompt in admin mode and run the below command.

```
Console

Netsh trace start scenario=netconnection capture=yes
tracefile=c:\Server.etl
```

5. Open the *server.etl* file with Network Monitor and in the filter section, apply the filter `Wscore_MicrosoftWindowsWinsockAFD.AFD_EVENT_BIND.Status.LENTStatus.Code == 0x209`. You should see entries that say **STATUS_TOO_MANY_ADDRESSES**. If you don't find any entries, then the server is still not out of ports. If you find them, then you can confirm that the server is under port exhaustion.

Troubleshoot Port exhaustion

The key is to identify which process or application is using all the ports. Below are some of the tools that you can use to isolate to one single process

Method 1

Start by looking at the netstat output. If you're using Windows 10 or Windows Server 2016, then you can run the command `netstat -anobq` and check for the process ID that has maximum entries as BOUND. Alternately, you can also run the below PowerShell command to identify the process:

```
PowerShell

Get-NetTCPConnection | Group-Object -Property State, OwningProcess | Select
-Property Count, Name, @{Name="ProcessName";Expression={(Get-Process -PID
($_.Name.Split(',')[-1].Trim(' '))).Name}}, Group | Sort Count -Descending
```

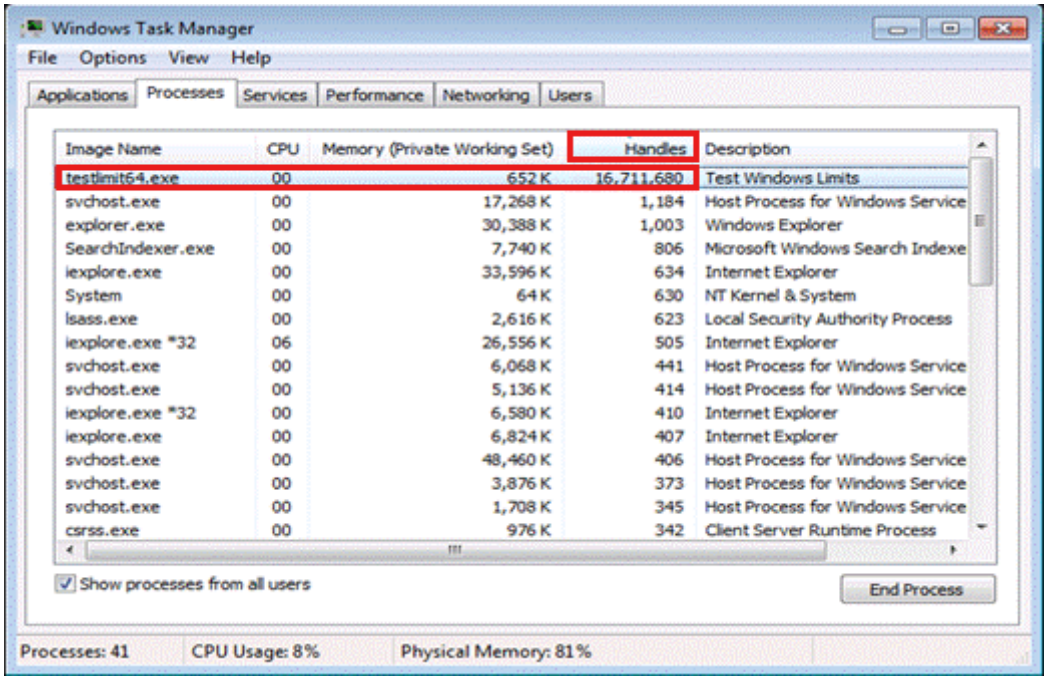
Most port leaks are caused by user-mode processes not correctly closing the ports when an error was encountered. At the user-mode level, ports (actually sockets) are handles. Both **TaskManager** and **ProcessExplorer** are able to display handle counts, which allows you to identify which process is consuming all of the ports.

For Windows 7 and Windows Server 2008 R2, you can update your PowerShell version to include the above cmdlet.

Method 2

If method 1 doesn't help you identify the process (prior to Windows 10 and Windows Server 2012 R2), then have a look at Task Manager:

1. Add a column called "handles" under details/processes.
2. Sort the column handles to identify the process with the highest number of handles. Usually the process with handles greater than 3000 could be the culprit except for processes like System, *lsass.exe*, *store.exe*, *sqlsvr.exe*.



3. If any other process than these processes has a higher number, stop that process and then try to sign in using domain credentials and see if it succeeds.

Method 3

If Task Manager didn't help you identify the process, then use Process Explorer to investigate the issue.

Steps to use Process explorer:

1. Download Process Explorer and run it **Elevated**.
2. Alt + select the column header, select **Choose Columns**, and on the **Process Performance** tab, add **Handle Count**.

3. Select **View** > **Show Lower Pane**.

4. Select **View** > **Lower Pane View** > **Handles**.

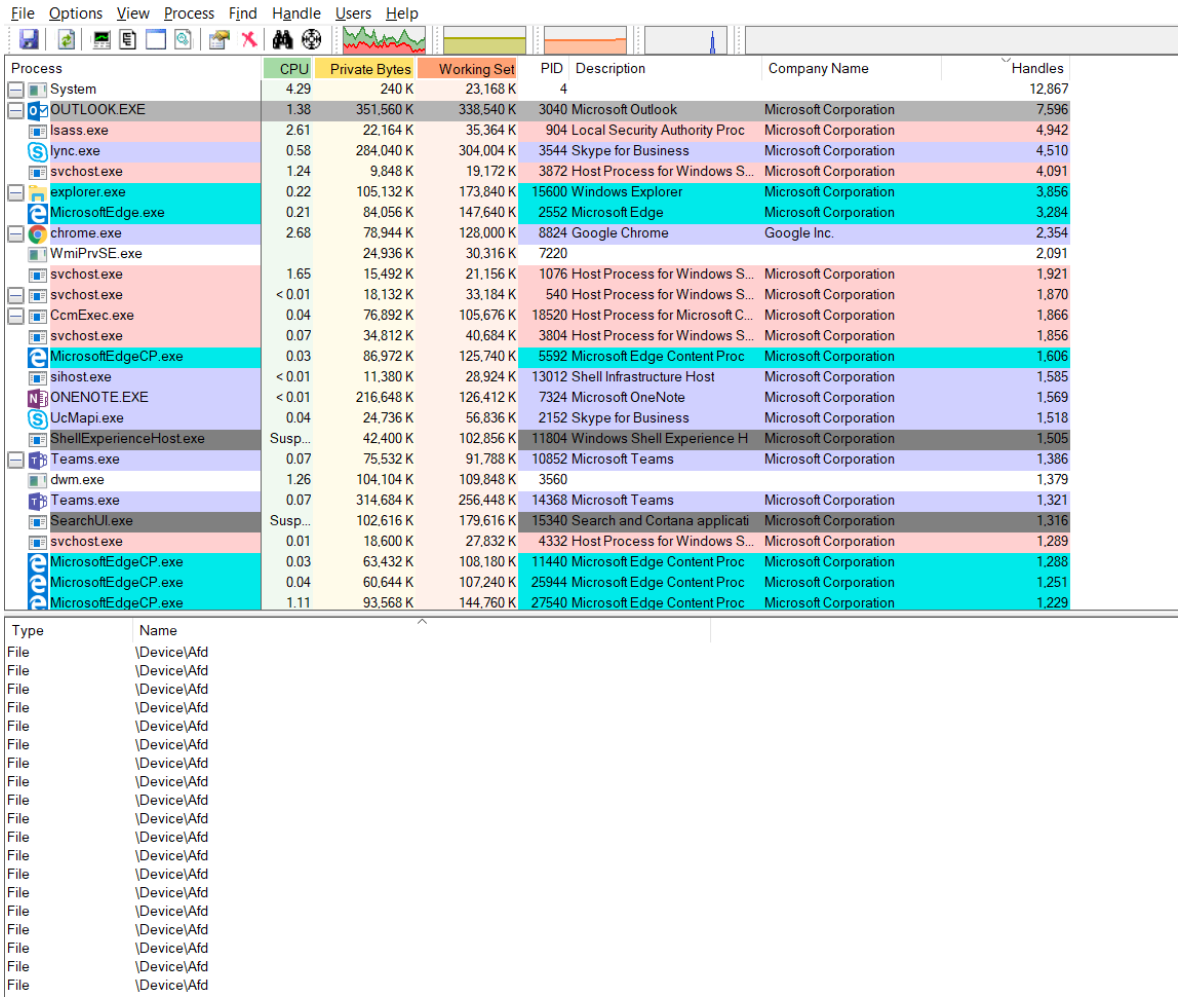
5. Select the **Handles** column to sort by that value.

6. Examine the processes with higher handle counts than the rest (will likely be over 10,000 if you can't make outbound connections).

7. Click to highlight one of the processes with a high handle count.

8. In the lower pane, the handles listed as below are sockets. (Sockets are technically file handles).

   File \Device\AFD



9. Some are normal, but large numbers of them aren't (hundreds to thousands). Close the process in question. If that restores outbound connectivity, then you've further proven that the app is the cause. Contact the vendor of that app.

Finally, if the above methods didn't help you isolate the process, we suggest you collect a complete memory dump of the machine in the issue state. The dump will tell you which process has the maximum handles.

As a workaround, rebooting the computer will get it back in normal state and would help you resolve the issue for the time being. However, when a reboot is impractical, you can also consider increasing the number of ports on the machine using the below commands:

Console

```
netsh int ipv4 set dynamicport tcp start=10000 num=1000
```

This command will set the dynamic port range to start at port 10000 and to end at port 10999 (1000 ports). The minimum range of ports that can be set is 255. The minimum start port that can be set is 1025. The maximum end port (based on the range being configured) can't exceed 65535.

> **Note**
>
> Note that increasing the dynamic port range is not a permanent solution but only temporary. You'll need to track down which process/processors are consuming max number of ports and troubleshoot from that process standpoint as to why it's consuming such high number of ports.

For Windows 7 and Windows Server 2008 R2, you can use the below script to collect the netstat output at defined frequency. From the outputs, you can see the port usage trend.

Console

```
@ECHO ON
set v=%1
:loop
set /a v+=1
ECHO %date% %time% >> netstat.txt
netstat -ano >> netstat.txt

PING 1.1.1.1 -n 1 -w 60000 >NUL

goto loop
```

More information

- Port Exhaustion and You! - this article gives a detail on netstat states and how you can use netstat output to determine the port status

- Detecting ephemeral port exhaustion: this article has a script that will run in a loop to report the port status. (Applicable for Windows 2012 R2, Windows 8, Windows 10 and Windows 11)

Troubleshoot TCP/IP connectivity

Article • 09/02/2022 • 5 minutes to read

Applies to: Windows 10

You might come across connectivity errors on the application end or timeout errors. The following are the most common scenarios:

- Application connectivity to a database server
- SQL timeout errors
- BizTalk application timeout errors
- Remote Desktop Protocol (RDP) failures
- File share access failures
- General connectivity

When you suspect that the issue is on the network, you collect a network trace. The network trace would then be filtered. During troubleshooting connectivity errors, you might come across TCP reset in a network capture that could indicate a network issue.

- TCP is defined as connection-oriented and reliable protocol. One of the ways in which TCP ensures reliability is through the handshake process. Establishing a TCP session would begin with a three-way handshake, followed by data transfer, and then a four-way closure. The four-way closure where both sender and receiver agree on closing the session is termed as graceful closure. After the four-way closure, the server will allow 4 minutes of time (default), during which any pending packets on the network are to be processed, this period is the TIME_WAIT state. After the TIME_WAIT state completes, all the resources allocated for this connection are released.
- TCP reset is an abrupt closure of the session; it causes the resources allocated to the connection to be immediately released and all other information about the connection is erased.
- TCP reset is identified by the RESET flag in the TCP header set to 1.

A network trace on the source and the destination helps you to determine the flow of the traffic and see at what point the failure is observed.

The following sections describe some of the scenarios when you'll see a RESET.

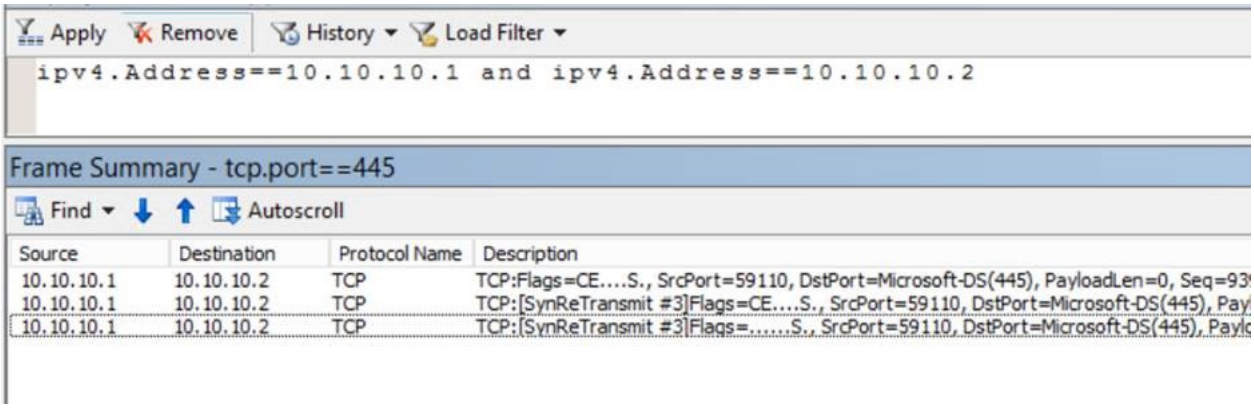
Packet drops

When one TCP peer is sending out TCP packets for which there's no response received from the other end, the TCP peer would end up retransmitting the data and when there's no response received, it would end the session by sending an ACK RESET (this ACK RESET means that the application acknowledges whatever data is exchanged so far, but because of packet drop, the connection is closed).

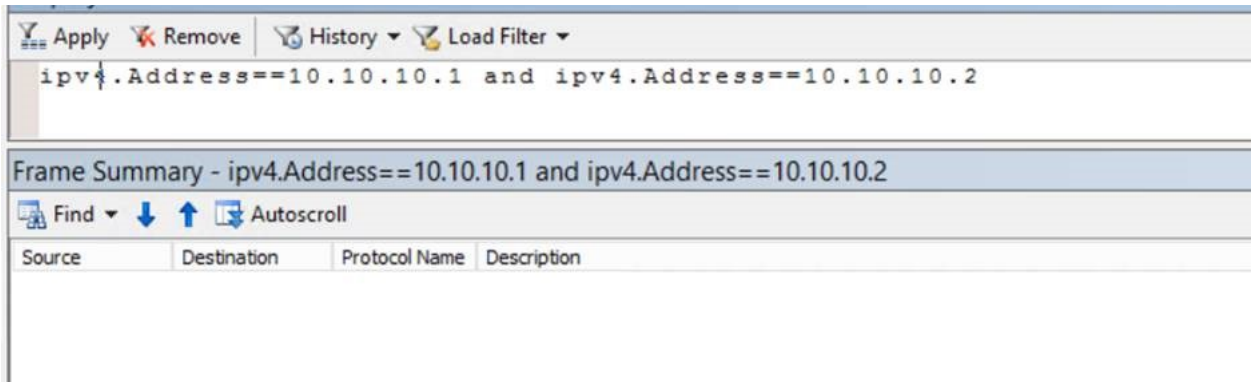
The simultaneous network traces on source and destination will help you verify this behavior where on the source side you would see the packets being retransmitted and on the destination none of these packets are seen. This scenario denotes that the network device between the source and destination is dropping the packets.

If the initial TCP handshake is failing because of packet drops, then you would see that the TCP SYN packet is retransmitted only three times.

Source side connecting on port 445:

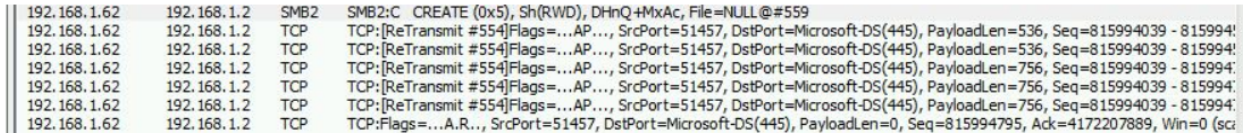


Destination side: applying the same filter, you don't see any packets.



For the rest of the data, TCP will retransmit the packets five times.

Source 192.168.1.62 side trace:



Destination 192.168.1.2 side trace:

You wouldn't see any of the above packets. Engage your network team to investigate with the different hops and see if any of them are potentially causing drops in the network.

If you're seeing that the SYN packets are reaching the destination, but the destination is still not responding, then verify if the port that you're trying to connect to is in the listening state. (Netstat output will help). If the port is listening and still there's no response, then there could be a wfp drop.

Incorrect parameter in the TCP header

You see this behavior when the packets are modified in the network by middle devices and TCP on the receiving end is unable to accept the packet, such as the sequence number being modified, or packets being replayed by middle device by changing the sequence number. Again, the simultaneous network trace on the source and destination will be able to tell you if any of the TCP headers are modified. Start by comparing the source trace and destination trace, you'll be able to notice if there's a change in the packets itself or if any new packets are reaching the destination on behalf of the source.

In this case, you'll again need help from the network team to identify any device that's modifying packets or replaying packets to the destination. The most common ones are RiverBed devices or WAN accelerators.

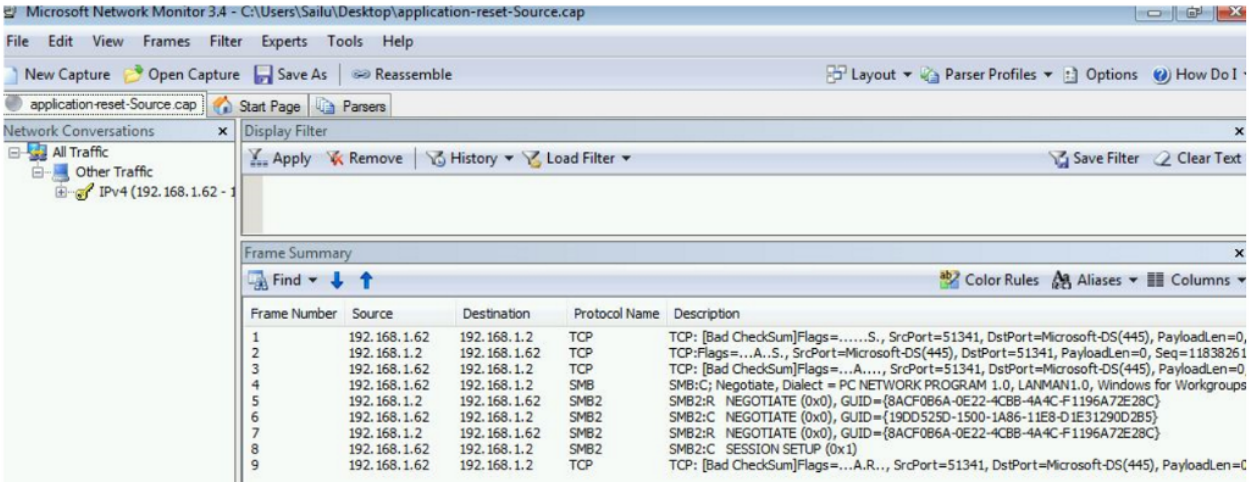
Application side reset

When you've identified that the resets aren't due to retransmits or incorrect parameter or packets being modified with the help of network trace, then you've narrowed it down to application level reset.

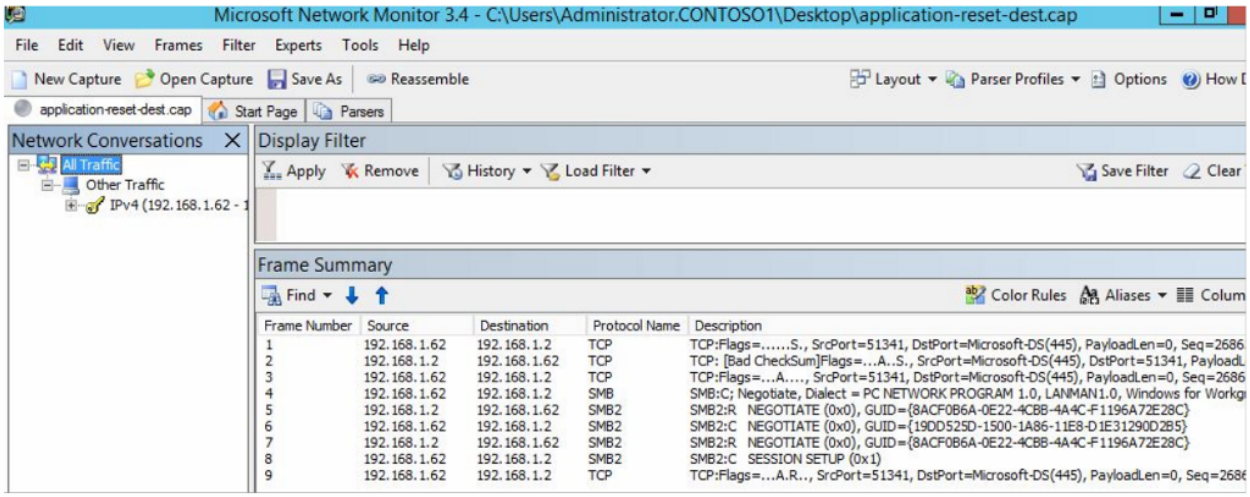
The application resets are the ones where you see the Acknowledgment flag set to 1 along with the reset flag. This setting would mean that the server is acknowledging the receipt of the packet but for some reason it will not accept the connection. This stage is when the application that received the packet didn't like something it received.

In the below screenshots, you see that the packets seen on the source and the destination are the same without any modification or any drops, but you see an explicit reset sent by the destination to the source.

Source Side



On the destination-side trace



You also see an ACK+RST flag packet in a case when the TCP establishment packet SYN is sent out. The TCP SYN packet is sent when the client wants to connect on a particular port, but if the destination/server for some reason doesn't want to accept the packet, it would send an ACK+RST packet.

Source	Destination	Protocol ...	Description
10.10.10.1	10.10.10.2	TCP	TCP:Flags=.....S., SrcPort=4434, DstPort=4437, PayloadLen=0, Seq=873742159, Ack=0, Win=8188 ...
10.10.10.2	*10.10.10.1*	*TCP*	*TCP: [Bad CheckSum]Flags=...A.R.., SrcPort=4437, DstPort=4434, PayloadLen=0, Seq=0, Ack=873...*

The application that's causing the reset (identified by port numbers) should be investigated to understand what is causing it to reset the connection.

> ⓘ **Note**
>
> The above information is about resets from a TCP standpoint and not UDP. UDP is a connectionless protocol and the packets are sent unreliably. You wouldn't see retransmission or resets when using UDP as a transport protocol. However, UDP makes use of ICMP as a error reporting protocol. When you've the UDP packet sent out on a port and the destination does not have port listed, you'll see the

destination sending out **ICMP Destination host unreachable: Port unreachable** message immediately after the UDP packet.

Output

```
10.10.10.1  10.10.10.2  UDP UDP:SrcPort=49875,DstPort=3343

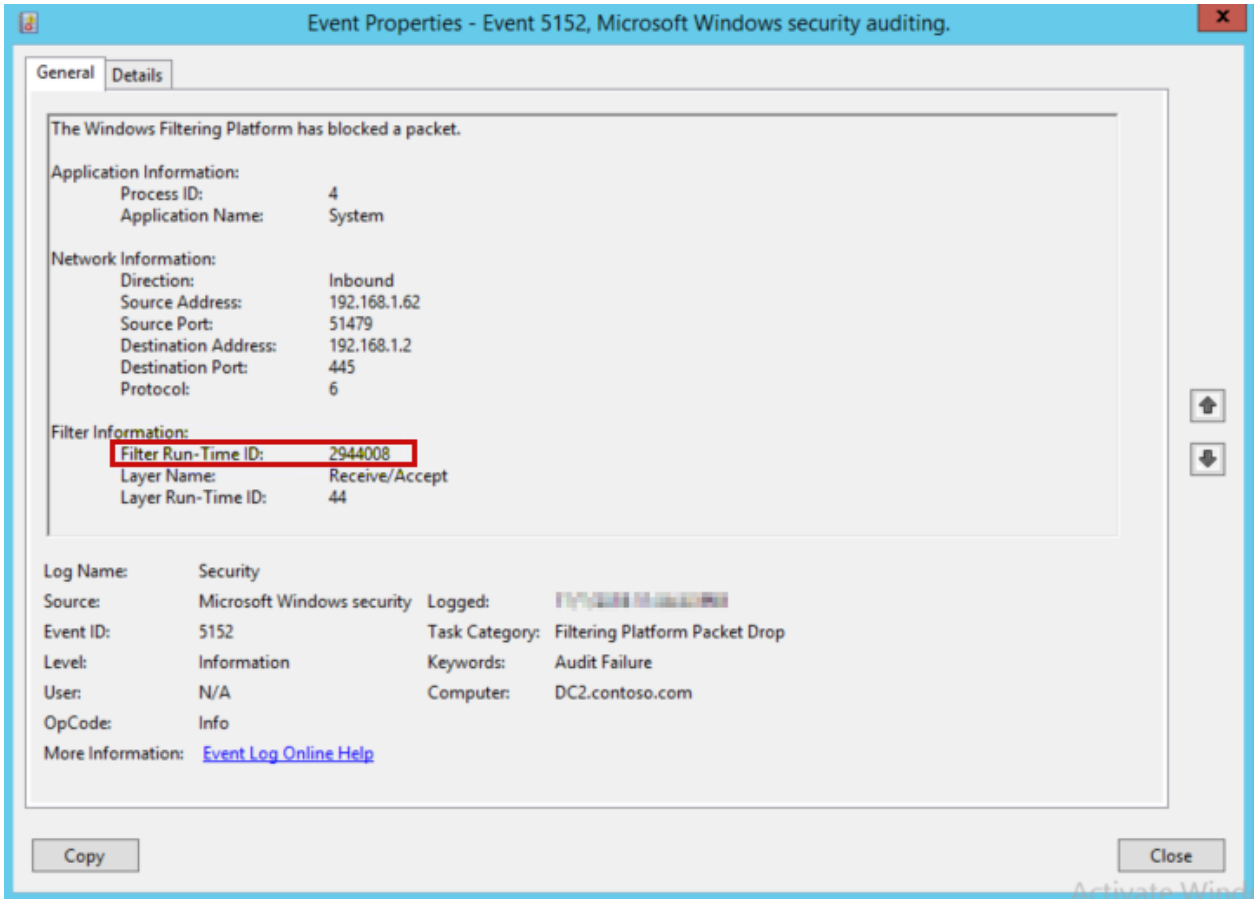
10.10.10.2  10.10.10.1  ICMP    ICMP:Destination Unreachable Message, Port
Unreachable,10.10.10.2:3343
```

During the troubleshooting connectivity issue, you might also see in the network trace that a machine receives packets but doesn't respond to. In such cases, there could be a drop at the server level. To understand whether the local firewall is dropping the packet, enable the firewall auditing on the machine.

Console

```
auditpol /set /subcategory:"Filtering Platform Packet Drop" /success:enable
/failure:enable
```

You can then review the Security event logs to see for a packet drop on a particular port-IP and a filter ID associated with it.



Now, run the command `netsh wfp show state`, this execution will generate a *wfpstate.xml* file. After you open this file and filter for the ID that you find in the above event (2944008), you'll be able to see a firewall rule name that's associated with this ID that's blocking the connection.



Collect data using Network Monitor

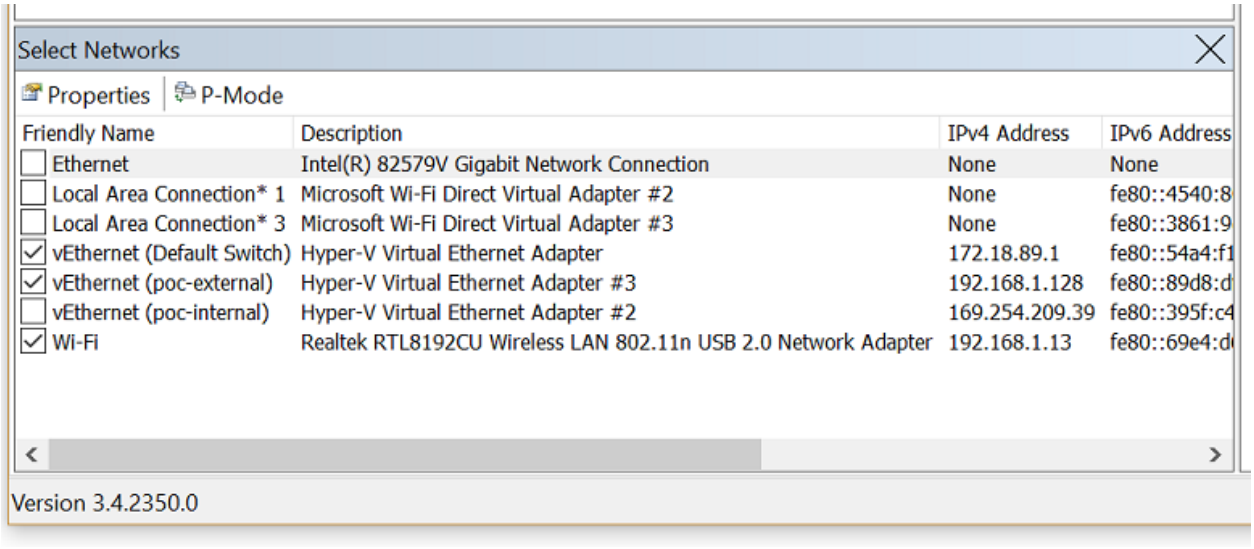
Article • 09/02/2022 • 2 minutes to read

In this article, you'll learn how to use Microsoft Network Monitor 3.4, which is a tool for capturing network traffic.

Applies to: Windows 10

> **Note**
>
> Network Monitor is the archived protocol analyzer and is no longer under development. Also, Microsoft Message Analyzer (MMA) was retired and its download packages were removed from microsoft.com sites on November 25, 2019. There is currently no Microsoft replacement for Microsoft Message Analyzer in development at this time. For similar functionality, consider using another, non-Microsoft network protocol analyzer tool. For more information, see **Microsoft Message Analyzer Operating Guide**.

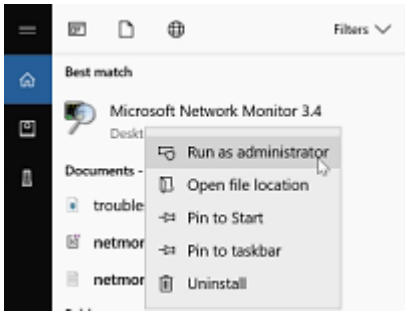
To get started, download Network Monitor tool. When you install Network Monitor, it installs its driver and hooks it to all the network adapters installed on the device. You can see the same on the adapter properties, as shown in the following image:



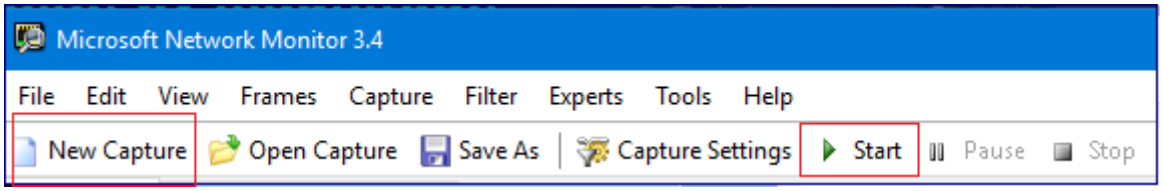
When the driver gets hooked to the network interface card (NIC) during installation, the NIC is reinitialized, which might cause a brief network glitch.

To capture traffic

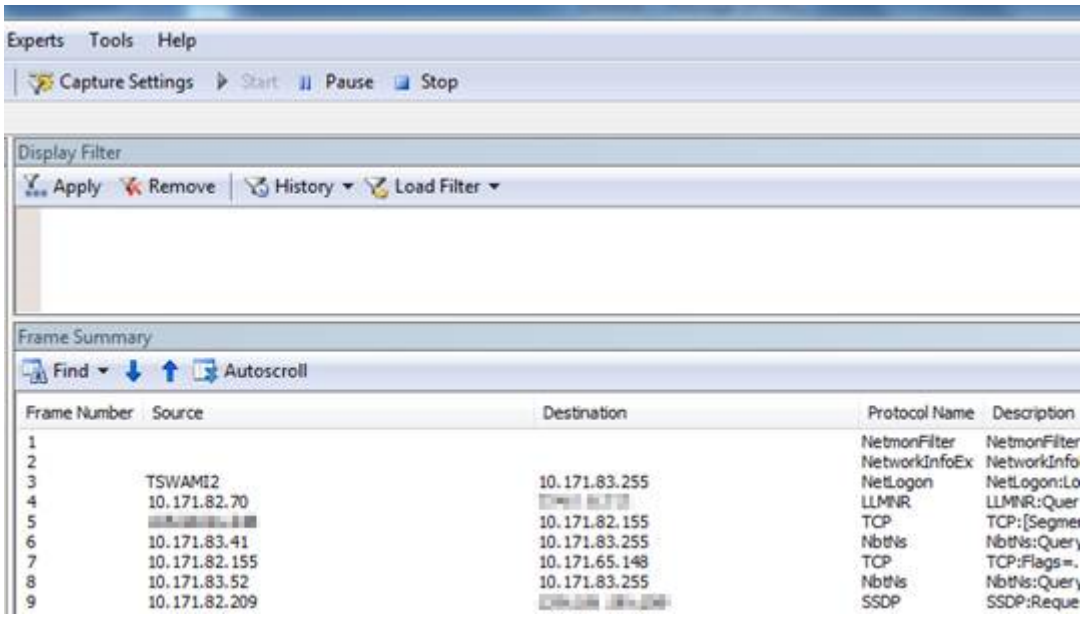
1. Run `netmon` in an elevated status by choosing **Run as Administrator**.



2. Network Monitor opens with all network adapters displayed. Select the network adapters where you want to capture traffic, select **New Capture**, and then select **Start**.



3. Reproduce the issue, and you'll see that Network Monitor grabs the packets on the wire.



4. Select **Stop**, and go to **File** > **Save as** to save the results. By default, the file will be saved as a `.cap` file.

The saved file has captured all the traffic that is flowing to and from the selected network adapters on the local computer. However, your interest is only to look into the traffic/packets that are related to the specific connectivity problem you're facing. So you'll need to filter the network capture to see only the related traffic.

Commonly used filters

- Ipv4.address=="client ip" and ipv4.address=="server ip"
- Tcp.port==
- Udp.port==
- Icmp
- Arp
- Property.tcpretranmits
- Property.tcprequestfastretransmits
- Tcp.flags.syn==1

> **Tip**
>
> If you want to filter the capture for a specific field and do not know the syntax for that filter, just right-click that field and select **Add the selected value to Display Filter**.

Network traces that are collected using the `netsh` commands built in to Windows are of the extension "ETL". However, these ETL files can be opened using Network Monitor for further analysis.

More information

- Intro to Filtering with Network Monitor 3.0
- Network Monitor Filter Examples
- Network Monitor Wireless Filtering
- Network Monitor TCP Filtering
- Network Monitor Conversation Filtering
- How to setup and collect network capture using Network Monitor tool

Additional default gateways may appear in persistent routes when you use LBFO

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where additional default gateways appear in persistent routes when you use Load Balancing and Failover (LBFO).

Applies to: Windows Server 2012 R2
Original KB number: 2966111

Symptoms

Assume that a network adapter is configured with IP settings that include a default gateway. Later, an LBFO team is created that includes the previously configured network adapter. The newly created teamed network adapter is configured with IP settings. In this situation, you may see the previously configured default gateway route and the newly configured default gateway route in the "Persistent Route" section of the Route Print command output.

For example, if an adapter is configured with a default gateway of 10.0.0.1, and it is then added to an LBFO teamed adapter that is configured with a default gateway of 192.168.0.1, both default routes may appear under the "Persistent Route" section of the Route Print command output as shown here:

```
===========================================================================
===========================
Persistent Routes:
Network Address          Netmask  Gateway Address  Metric
0.0.0.0                  0.0.0.0        10.0.0.1  Default
0.0.0.0                  0.0.0.0      192.168.0.1  Default
===========================================================================
===========================
```

However, in the "Active Routes" section of the Route Print command output, only the newly configured LBFO teamed adapter default gateway is present.

Cause

This behavior is by design. The legacy route.exe tool does not indicate to which interface the routes in the "Persistent Routes" section are related. The Route Print command shows routes from the active network configuration store in the "Active Routes" section of the command output, and from the persistent network configuration store in the "Persistent Routes" section of the command output. However, the route.exe tool does not indicate to which adapter a persistent route belongs. Because the routes from the previously configured adapter are not in the active route table, there is no functional impact upon the active routing table or the networking behavior.

Resolution

We recommend that you use the Get-NetRoute PowerShell cmdlet when clarity is needed about which routes are in the active store or persistent store, and to which adapters routes apply.

The Get-NetRoute PowerShell cmdlet allows for the administrator to see specifically what is stored in each networking configuration store and to which interface the route belongs.

For the persistent store:

```
PowerShell

Get-NetRoute -AddressFamily IPv4 -PolicyStore PersistentStore
```

For the active store:

```
PowerShell

Get-NetRoute -AddressFamily IPv4 -PolicyStore ActiveStore
```

Can't install the SNMP and WMI SNMP Provider features in Windows 10 or Windows 11

Article • 11/24/2021 • 2 minutes to read

This article provides workarounds to install the Simple Network Management Protocol (SNMP) and Windows Management Instrumentation (WMI) SNMP Provider features in Windows 10 or Windows 11.

Error when installing the SNMP and WMI SNMP Provider features

You try to install the SNMP and WMI SNMP Provider features in Windows 10 or Windows 11 by using the Deployment Image Servicing and Management (DISM.exe) tool as follows:

Console

```
dism /online /enable-feature /featureName:SNMP /featureName:WMISnmpProvider
```

Then, you receive this error message:

> Error: 0x800f080c
> Feature name SNMP is unknown.
> Feature name WMISnmpProvider is unknown.
> A Windows feature name was not recognized.
> Use the /Get-Features option to find the name of the feature in the image and try the command again.

> **Important**
>
> This issue occurs because the SNMP and WMI SNMP Provider features are deprecated.

To work around this issue, use one of the following methods.

Install the SNMP and WMI SNMP Provider features from the Settings page

1. Go to Start, select **Settings** > **Apps**.
2. Under **Apps & features**, select **Optional features** > **Add a feature**.

    - To install the SNMP feature, select **Simple Network Management Protocol (SNMP)** > **Install**.
    - To install the WMI SNMP Provider feature, select **WMI SNMP Provider** > **Install**.

To verify the installation state, select **See optional features history**.

Install the SNMP and WMI SNMP Provider features by using Windows PowerShell

1. Start Windows PowerShell as an administrator.

2. Run the following Add-WindowsCapability cmdlets to install the SNMP and WMI SNMP Provider features.

    ```
    PowerShell

    Add-WindowsCapability -Online -Name "SNMP.Client~~~~0.0.1.0"
    ```

    ```
    PowerShell

    Add-WindowsCapability -Online -Name "WMI-SNMP-
    Provider.Client~~~~0.0.1.0"
    ```

To verify the installation state, run the following Get-WindowsCapability cmdlets.

```
PowerShell

Get-WindowsCapability -Online -Name "SNMP.Client~~~~0.0.1.0"
```

```
PowerShell

Get-WindowsCapability -Online -Name "WMI-SNMP-Provider.Client~~~~0.0.1.0"
```

The state is **Installed** if these features are installed correctly.

You can't turn on Network Discovery in Network and Sharing Center

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution for the issue that you can't turn on Network Discovery in Network and Sharing Center.

Applies to: Windows Server 2012 R2
Original KB number: 2722035

Symptoms

You try to turn on Network Discovery on a computer that's running Windows Server 2012. To do it, you change the Advanced sharing settings in **Network and Sharing Center**. However, the changes aren't saved. So you can't turn on Network Discovery. And you experience the following issues:

- You can't browse or find any network share.
- You can't view shared folders on a local network.

Cause

This issue occurs for one of the following reasons:

- The dependency services for Network Discovery aren't running.
- The Windows firewall or other firewalls don't allow Network Discovery.

Resolution

To resolve the issue, follow these steps:

1. Make sure that the following dependency services are started:

    - DNS Client
    - Function Discovery Resource Publication
    - SSDP Discovery
    - UPnP Device Host

2. Configure the Windows firewall to allow Network Discovery by following these steps:

a. Open **Control Panel**, select **System and Security**, and then select **Windows Firewall**.
b. In the left pane, select **Allow an app or feature through Windows Firewall**.
c. Select **Change settings**. If you're prompted for an administrator password or confirmation, enter the password or provide confirmation.
d. Select **Network discovery**, and then select **OK**.

3. Configure other firewalls in the network to allow Network Discovery.

4. Turn on **Network Discovery** in **Network and Sharing Center**.

How to use Ping.exe to check your Microsoft Broadband Network Adapter

Article • 09/23/2021 • 2 minutes to read

This article provides some information about checking your Microsoft Broadband Network Adapter with Ping.exe.

Applies to: Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 814155

Summary

This article describes how to use the Microsoft Windows Ping.exe utility to determine if your network adapter is working.

More information

To use ping effectively, you need the following information:

- The IP address of the network adapter that you are checking.
- The IP address of your default gateway. It may be your base station, modem, or router, depending on how your network is configured.

To find this information:

1. Click **Start**, click **Run**, type cmd, and then click **OK**.
2. At the command prompt, type ipconfig, and then press ENTER.
3. Note the following information:
    - The IP address of the network adapter that you want to check.
    - The IP address of your default gateway.

Use Ping.exe to Check Your Hardware

To do this checking:

1. At the command prompt, type ping loopback /localhost 127.0.0.1, and then press ENTER. The result should be similar as:

```
Console

Reply from 127.0.0.1: bytes=127 time<1ms TTL=128
Reply from 127.0.0.1: bytes=127 time<1ms TTL=128
Reply from 127.0.0.1: bytes=127 time<1ms TTL=128
Reply from 127.0.0.1: bytes=127 time<1ms TTL=128
```

Ping statistics for 127.0.0.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round-trip times in milliseconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
If it does not work, there may be a problem with TCP/IP on your computer. You may have to reinstall TCP/IP, and you cannot complete the following steps until you can successfully complete this step.

2. At the command prompt, type ping **network_adapter_IP_address**, and then press ENTER. For example, if your network adapter's IP address is 192.168.2.9, type ping 192.168.2.9, and then press ENTER. The result should be similar to the as:

```
Console

Reply from 192.168.2.9: bytes=32 time<1ms TTL=128
Reply from 192.168.2.9: bytes=32 time<1ms TTL=128
Reply from 192.168.2.9: bytes=32 time<1ms TTL=128
Reply from 192.168.2.9: bytes=32 time<1ms TTL=128
```

Ping statistics for 192.168.2.9: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round-trip times in milliseconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
If it does not work, there may be a problem with your network adapter.

3. At the command prompt, type ping **gateway_IP_address**, and then press ENTER. For example, if the IP address of your base station is 192.168.2.1, type ping 192.168.2.1, and then press ENTER. The result should be similar to the as:

```
Console

Reply from 192.168.2.1: bytes=32 time=5ms TTL=64
Reply from 192.168.2.1: bytes=32 time=4ms TTL=64
Reply from 192.168.2.1: bytes=32 time=4ms TTL=64
Reply from 192.168.2.1: bytes=32 time=4ms TTL=64
```

Ping statistics for 192.168.2.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round-trip times in milliseconds: Minimum = 4 ms, Maximum = 5 ms,

Average = 4 ms

If it does not work, there may be a problem with your base station, modem, router, or network cable.

References

For additional information about how to troubleshoot TCP/IP in Microsoft Windows, click the following article numbers to view the articles in the Microsoft Knowledge Base:

314067 How to troubleshoot TCP/IP connectivity with Windows XP

169790 How to troubleshoot basic TCP/IP problems

Devices can't connect to mobile broadband after over-the-air update from mobile operator

Article • 12/06/2021 • 2 minutes to read

This article provides a resolution for the issue that devices can't connect to mobile broadband after over-the-air update from mobile operator.

Applies to: Windows 10 - all editions
Original KB number: 3160433

Symptoms

Your Windows 10-based device could connect to mobile broadband in the past, but connection attempts fail after your mobile operator applies an over-the-air update to your device. This problem affects only enterprise customers who have special plans with their mobile operator partners.

Cause

This problem occurs if the mobile operator made an over-the-air update directly to your modem. Windows tries to make a connection by using the configurations in the operating system based on previous successful connections. However, the mobile operator network and modem may block the connection request from Windows because of the mismatch between the Windows request and the configuration in the modem.

Resolution

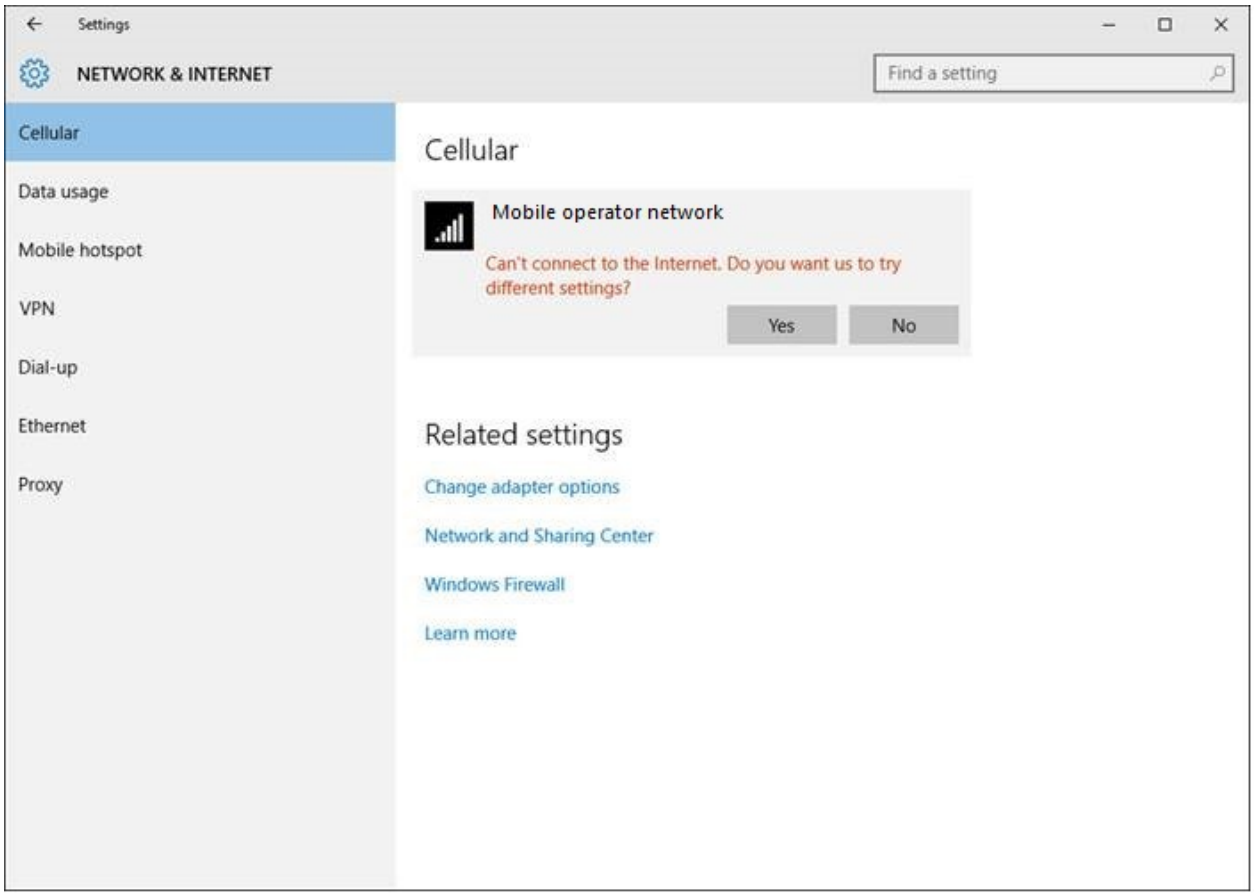
> ⚠ **Warning**
>
> Before you apply the following method, check your version of Windows to make sure that you're running Windows 10, build 10586.420 or later. To do this, press the Window key + R, and then type winver . If you're not running build 10586.420 or later, update your Windows installation to the latest available version.

To resolve the issue that's described in the "Symptoms" section, follow these steps:

1. Open Registry Editor by pressing the Windows Key + R and then typing regedit.
2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\Settings\Network.
3. Right-click the **Network** key, and then click **Permissions**.
4. Click **Advanced**, and check whether the owner is **TrustedInstaller**.
5. Click the "Change" link, and then enter < **machine_name** >\Administrators.
6. Click **Check Names** to verify that < **machine_name** >\Administrators is correctly validated (underlined). For example: *MY-LAPTOP\Administrators*. If it is, click **OK**.

   If **Check Names** does not return an underlined name, your user name is not in the correct format.
7. Click **OK** in the **Advanced Security Settings for Network** pane.
8. Select **Administrators**, select the **Full Control** check box in the **Allow** column, and then click **OK**.
9. Create or locate the following registry key, and set the DWORD value to 1 (DWORD=1):

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Control Panel\Settings\Network\ManualConnectionRetry`
10. Go to **Settings** -> **Network and Internet** -> **Cellular** -> **Connect**.
11. A retry page that resembles as:



12. Click **Yes**.

    Windows can now connect by using the configuration in the modem. This modem configuration overwrites the existing configuration on the operating system.

Windows 10: Enterprise APN lost after SIM change or MBN adapter error

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue that enterprise APN lost after SIM change or MBN adapter error.

Applies to: Windows 10 - all editions
Original KB number: 4487376

Symptoms

A Windows 10 client that previously connected to the enterprise wireless network can no longer connect after the SIM was removed or the MBN adapter encountered an error or failure, even if the SIM or MBN adapter is now working correctly.

This situation applies if the wireless connection, including the enterprise access point name (APN), was configured at the time of provisioning by using either of the following methods:

- Using a provisioning package that was built by using Windows Configuration Designer (for more information, see Configure cellular settings for tablets and PCs)
- Using the following command at the Windows command prompt:

```
Console

netsh mbn add profile interface="MBN IF name" name="path to
profile.xml"
```

The initial provisioning successfully created a profile.xml file that listed the enterprise APN. However, after the SIM was removed or after the MBN adapter experienced an error or failure (for example, after a power transition occurred), the computer can no longer use the enterprise APN. The `netsh mbn show profile` command cannot show the profile information. This is because the profile.xml file has been deleted.

Cause

Windows 10 manages enterprise APNs in the same manner that it manages OEM-provisioned APNs: It associates the APN with the SIM. If the SIM is removed, so is the

APN.

Resolution

To configure a Windows 10 client to associate the APN with any SIM that is used on the MBN adapter, you must create a new provisioning package that includes a customized answer file.

> **ⓘ Important**
>
> To make these modifications, you must edit the answer file manually, and use the Windows Configuration Designer command-line interface (CLI) to rebuild the provisioning package. For more information about how to use the Windows Designer CLI, see **Windows Configuration Designer command-line interface (reference)**.

The process of customizing the APN configuration resembles the process that is described in Create a provisioning package with multivariant settings. However, instead of creating variants of a configuration for variants in hardware, you define a wildcard to apply the same configuration to any hardware.

Example

Consider the following segment of an answer file:

XML

```
<Customizations>
  <Common>
    <Connections>
      <EnterpriseAPN>
        <EnterpriseConnection EnterpriseConnectionName="Contoso"
Name="Contoso">
          <APNName>Contoso</APNName>
          <AlwaysOn>True</AlwaysOn>
          <AuthType>None</AuthType>
          <Enabled>True</Enabled>
        </EnterpriseConnection>
      </EnterpriseAPN>
    </Connections>
  </Common>
</Customizations>
```

To support any SIM, edit the answer file segment as follows:

XML

```
<Settings xmlns="urn:schemas-microsoft-com:windows-provisioning">
  <Customizations>
    <Targets>
      <Target Id="AnyUicc">
        <TargetState>
          <Condition Name="iccid" Value="pattern:.*" />
        </TargetState>
      </Target>
    </Targets>
    <Variant>
     <TargetRefs>
       <TargetRef Id="AnyUicc" />
     </TargetRefs>
     <Settings>
       <Connections>
         <EnterpriseAPN>
           <EnterpriseConnection EnterpriseConnectionName="Contoso"
Name="Contoso">
             <APNName>Contoso</APNName>
             <AlwaysOn>True</AlwaysOn>
           </EnterpriseConnection>
         </EnterpriseAPN>
       </Connections>
     </Settings>
    </Variant>
  </Customizations>
</Settings>
```

To rebuild the provisioning package that contains the edited answer file, run the following command:

Console

```
Icd.exe /build-provisioningpackage
/CustomizationXML:c:\temp\enterprise_anysim.xml
/PackagePath:x:\ppkgs\enterprise_anysim [optional /StoreFile:Microsoft-
Desktop-Provisioning.dat] +Overwrite
```

References

- Windows Configuration Designer command-line interface (reference)
- Configure cellular settings for tablets and PCs
- How to Create a provisioning package with multivariant settings

You receive the error 'WSAENOBUFS (10055)' when you try to connect from TCP ports greater than 5000

Article • 09/23/2021 • 3 minutes to read

This article helps to fix the error 'WSAENOBUFS (10055)' when you try to connect from TCP ports greater than 5000.

Applies to: Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 196271

Symptoms

If you try to set up TCP connections from ports that are greater than 5000, the local computer responds with the following WSAENOBUFS (10055) error message:

> An operation on a socket could not be performed because the system lacked sufficient buffer space or because a queue was full.

Resolution

Important

This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:
322756 How to back up and restore the registry in Windows

The default maximum number of ephemeral TCP ports is 5000 in the products that are included in the "Applies to" section. A new parameter has been added in these products. To increase the maximum number of ephemeral ports, follow these steps:

1. Start Registry Editor.

2. Locate the following subkey in the registry, and then click **Parameters:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

3. On the **Edit** menu, click **New**, and then add the following registry entry:
   Value Name: MaxUserPort
   Value Type: DWORD Value data: 65534 Valid Range: 5000-65534 (decimal) Default: 0x1388 (5000 decimal) Description: This parameter controls the maximum port number that is used when a program requests any available user port from the system. Typically, ephemeral (short-lived) ports are allocated between the values of 1024 and 5000 inclusive. After the release of security bulletin MS08-037, the behavior of Windows Server 2003 was changed to more closely match that of Windows Server 2008 and Windows Vista. For more information about Microsoft security bulletin MS08-037, click the following article numbers to view the articles in the Microsoft Knowledge Base:

   951746 MS08-037: Description of the security update for DNS in Windows Server 2008, in Windows Server 2003, and in Windows 2000 Server (DNS server-side): July 8, 2008

   951748 MS08-037: Description of the security update for DNS in Windows Server 2003, in Windows XP, and in Windows 2000 Server (client side): July 8, 2008

   953230 MS08-037: Vulnerabilities in DNS could allow spoofing

4. Exit Registry Editor, and then restart the computer.

> **Note**
>
> An additional TCPTimedWaitDelay registry parameter determines how long a closed port waits until the closed port can be reused.

More information

For more information about a related topic, visit the following Microsoft Web site:

https://technet.microsoft.com/library/bb726981.aspx
For more information about a related topic, click the following article numbers to view the articles in the Microsoft Knowledge Base:

314053 TCP/IP and NBT configuration parameters for Windows XP

Technical support for x64-based versions of Microsoft Windows

If your hardware came with a Microsoft Windows x64 edition already installed, your hardware manufacturer provides technical support and assistance for the Windows x64 edition. In this case, your hardware manufacturer provides support because a Windows x64 edition was included with your hardware. Your hardware manufacturer might have customized the Windows x64 edition installation by using unique components. Unique components might include specific device drivers or might include optional settings to maximize the performance of the hardware. Microsoft will provide reasonable-effort assistance if you must have technical help with a Windows x64 edition. However, you might have to contact your manufacturer directly. Your manufacturer is best qualified to support the software that your manufacturer installed on the hardware. If you purchased a Windows x64 edition such as a Windows Server 2003 x64 edition separately, contact Microsoft for technical support.

Error 0x80071779 when removing network components in Windows 10

Article • 12/06/2021 • 2 minutes to read

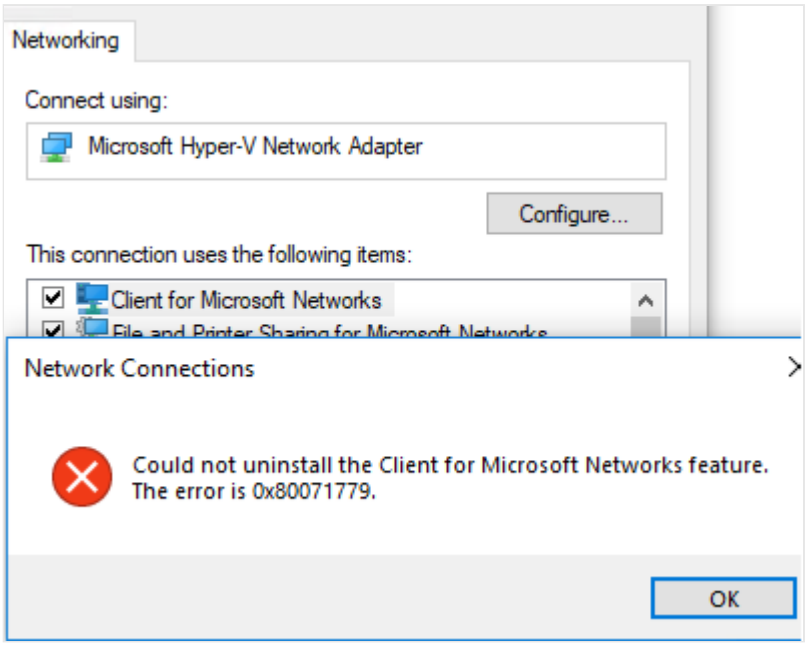
This article helps fix an error 0x80071779 that occurs when you uninstall the **Client for Microsoft Networks** or other network components.

Applies to: Window 10 – all editions
Original KB number: 4340181

Symptoms

Starting with Windows 10, version 1803 and newer based device or computer, you can't uninstall the **Client for Microsoft Networks** or other network components. You receive the following error message:

> Could not uninstall the Client for Microsoft Networks feature.
>
> The error is 0x80071779.



Cause

This behavior is by design.

Resolution

Microsoft doesn't support using this GUI or **netcfg** to uninstall protocols or built-in drivers. Instead, you can unbind the driver from Network Adapters either by using this GUI or the PowerShell cmdlet `Disable-NetAdapterBinding`. This is effectively the same as uninstalling the driver.

More information

If there are specific drivers that you want to remove but that are currently not part of an optional feature, file a feature request in the Feedback Hub.

Error when you try to establish a dial-up connection: Error 734: The PPP link control protocol was terminated

Article • 09/23/2021 • 2 minutes to read

This article helps fix an issue where **Error 734: The PPP link control protocol was terminated** occurs when you try to establish a dial-up connection.

Applies to: Windows 2000
Original KB number: 318718

Symptoms

If you try to establish a Point-to-Point Protocol (PPP) dial-up connection, you may receive the following error message:

> Error 734: The PPP link control protocol was terminated.

As a result, you can't establish a dial-up connection.

Cause

This issue may occur if either of the following conditions are true:

- Multi-link negotiation is turned on for the single-link connection.
- The dial-up connection security configuration is incorrectly configured to use the **Require secured password** setting.

Resolution

To resolve this issue:

1. Click **Start**, point to **Settings**, and then click **Network and Dial-up Connections**.

   > ⓘ **Note**
   >
   > For Windows Server 2003, click **Start**, point to **Control Panel**, and then point to **Network Connections**.

2. Right-click the appropriate dial-up networking connection, and then click **Properties**.
3. Click the **Networking** tab, and then click **Settings**.
4. Click to clear the **Negotiate multi-link for single link connections** check box (if it's selected).
5. Click **OK** > **OK**.
6. Double-click the connection, and then click **Dial**.
    - If this procedure resolves the issue and you can establish a dial-up connection, you don't have to follow the remaining steps in this article.
    - If this doesn't resolve the issue and you can't establish a dial-up connection, go to step 7 to continue to troubleshoot this issue.
7. Right-click the connection, and then click **Properties**.
8. Click the **Security** tab.
9. Under **Security options**, click **Allow unsecured password** in the **Validate my identity as follows** box, and then click **OK**.
10. Double-click the connection, and then click **Dial** to verify that you can establish a dial-up connection.

Information about power management setting on a network adapter

Article • 09/23/2021 • 4 minutes to read

This article provides a resolution to disable network adapter power management on a single computer.

Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
Original KB number: 2740020

Summary

The enhancements made to Windows 7 for managing power settings for network adapters greatly reduces the number of spurious wakes. It allows computers to sleep for longer periods of time when idle. Furthermore, you can configure the power management settings to meet the needs of your users through device properties, standard registry settings.

When deploying Windows 7 or Windows Server 2008 R2, you may want to disable the following network adapter power management setting on some computers:

Allow the computer to turn off this device to save power

More information

The **Allow the computer to turn off this device to save power** setting controls how the network card is handled when the computer enters sleep. This setting can be used if a driver misrepresents how it handles sleep states.

Windows never turns off the network card due to inactivity. When this setting is checked(enabled), Windows puts the network card to sleep and when it resumes it puts it back to D0. When this setting isn't checked(disabled), Windows completely halts the device and on resume reinitializes it. This setting is useful if a network card driver says it supports going to different sleep states and back to D0 but it ultimately doesn't support this functionality.

You can use Device Manager to change the power management settings for a network adapter. To disable this setting in **Device Manager**, expand **Network Adapters**, right-click the adapter, select **Properties**, select the **Power Management** tab, and then clear the **Allow the computer to turn off this device to save power** check box.

In Windows 7 or Windows Server 2008 R2, you have two additional check boxes on the **Power Management** tab for the Network Adapter that defines whether this device can wake the computer:

- Allow this device to wake the computer
- Only allow a magic packet to wake the computer

> ⓘ **Note**
>
> For above mentioned settings to work, you may also have to enable BIOS settings to enable WOL. The specific BIOS settings depend on the manufacturer of the computer.

However, with some Windows 7 or Windows Server 2008 R2 installations, you may want to use the registry to disable the **Allow the computer to turn off this device to save power** network adapter power management setting. Or you may want to use the registry to configure the wake options described above.

How to use Registry Editor to disable network adapter power management on a single computer

> ⓘ **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

To disable the network adapter power management setting for a single computer, follow these steps:

1. Select **Start**, select **Run**, type *regedit* in the **Open** box, and then select **OK**.
2. Locate and then select the following registry subkey:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}\DeviceNumber`

> ⓘ Note
>
> **DeviceNumber** is the network adapter number. If a single network adapter is installed on the computer, the **DeviceNumber** is **0001**.

3. Select **PnPCapabilities**.
4. On the **Edit** menu, select **Modify**.
5. In the **Value data** box, type *24*, and then select **OK**.

> ⓘ Note
>
> By default, a value of **0** indicates that power management of the network adapter is enabled. A value of **24** will prevent Windows 7 from turning off the network adapter or let the network adapter wake the computer from standby.

6. On the **File** menu, select **Exit**.

Additional information

You have three options for the power management properties of the Network Card:

- Option 1: Allow the computer to turn off this device to save power
- Option 2: Allow this device to wake the computer
- Option 3: Only allow a magic packet to wake the computer

The different possible combinations that exist along with their DWORD values (in decimal and hex) are:

- Option 1 and option 2 are checked, Option 3 is unchecked: This combination is default and hence its value is **0**.
- Option 1, option 2, and option 3 are all checked: The value becomes **0x100 (256)**.
- Only option 1 is checked: The value becomes **0x110 (272)**.
- Option 1 is unchecked (Note that option 2 and option 3 will be greyed out as a result): The value becomes **0x118 (280)**.

A conflict happens for the DWORD value for the last step where Option 1 is only checked, if the following steps are done exactly as mentioned below:

- If you check all the boxes, then the value is **256 (0x100)**.

- If you uncheck the box 1, the other two will be greyed out, and the value becomes **280 (0x118)**.
- If you check all the boxes except, the third one, PNPCapabilities value becomes **0**.
- If step 2 is repeated, the value becomes **24 (0x18)**.

Now, the values are different for the same setting because the way it has been achieved.

For deployment purpose, to keep option 1 cleared, one needs to use the value **24 (0x18)**. By default, option 1 and 2 are checked. It's the same as DWORD value **0** of this key, even though the key doesn't exist in the registry by default. Hence, creating this key with a value **24 (0x18)** in the deployment script/build process will inject this entry in the registry, which in turn should uncheck the first box during server startup.

In the same way, if you want to keep option 1 checked while option 2 and 3 cleared, the required value would be **10 (0x16)**.

> ⓘ **Note**
>
> This is entirely by design.

ICS doesn't work after computer or service restarts in Windows 10

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to issues where the Internet Connection Sharing (ICS) settings are lost and the ICS connection doesn't work after you restart the ICS service or the computer that runs Windows 10, version 1709.

Applies to: Windows 10, version 1709
Original KB number: 4055559

Symptoms

Consider the following scenario:

- You have a Windows 10, version 1709-based computer that has two network interfaces that connect to two different networks.
- You change the ICS service Startup type to **Automatic**.
- You enable ICS on one of the network interfaces and then confirm that ICS connection works.
- You restart the ICS service or the computer.

In this scenario, the ICS settings are lost, and the ICS connection doesn't work.

> **Note**
>
> Generally, if there is no traffic on ICS for 4 minutes, the service shuts down and does not restart automatically.

Resolution

> **Note**
>
> - Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

- This solution is currently available only in Windows 10 Version 1709 with update KB 4054517 installed.

To fix this issue, set the following registry subkey, and then change the ICS Service Startup mode to **Automatic**:

- Path: `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SharedAccess`
- Type: DWORD
- Setting: EnableRebootPersistConnection
- Value: 1

An Internet Explorer or Edge window opens when your computer connects to a corporate network or a public network

Article • 04/06/2022 • 7 minutes to read

This article provides some information about the issue where an Internet Explorer or Edge window opens when your computer connects to a corporate network or a public network.

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 4494446

Symptoms

You connect a computer that's running Windows 8 (or a later version) to a network in either of the following conditions:

- You connect your computer to a public network that requires Hotspot Sign in information (for example a hotel, airport, and so forth).
- You connect your computer to a corporate network that uses a proxy server to connect to the internet.

You notice the following behavior:

- The default browser (for example, **Internet Explorer** or **Edge**) opens, and shows a web page such as a sign-in page for the network or the MSN portal page.
- The network icon on the Task Bar shows an alert symbol (for example, ). If you hover over the icon, you see a message such as "No connectivity" or "Limited Internet access."

After you sign in to the network, you can use the network in the usual manner. After you use the network for a few seconds, the network alert on the Task Bar disappears.

Cause

This behavior is by design.

More information

Windows uses the Network Location Awareness (NLA) service to detect the properties of a network and determine how to manage connections to that network. NLA uses a component that is named the Network Connectivity Status Indicator (NCSI) to determine whether the computer has successfully connected to the network, and whether the network has intranet or internet connectivity.

NCSI uses both active and passive probes. These probes are triggered by changes in any of the network interfaces. When you connect your computer to a network as described in the Symptoms section, NCSI begins a process that includes one or more of the following:

- NCSI active probes and the network status alert
- Authentication and the automatic sign-in page
- NCSI passive monitoring and the network status alert

NCSI active probes and the network status alert

The active probe process consists of the following steps:

- Windows 10 or later versions:

    1. NCSI sends a DNS request to resolve the address of the `www.msftconnecttest.com` FQDN.

    2. If NCSI receives a valid response from a DNS server, NCSI sends a plain HTTP GET request to `http://www.msftconnecttest.com/connecttest.txt`.

    3. If NCSI successfully downloads the text file, it makes sure that the file contains Microsoft Connect Test.

    4. NCSI sends another DNS request to resolve the address of the `dns.msftncsi.com` FQDN.
        - If any of these requests fails, the network alert appears in the Task Bar (as described in Symptoms). If you hover over the icon, you see a message such as "No connectivity" or "Limited Internet access" (depending on which requests failed).
        - If all of these requests succeed, the Task Bar shows the usual network icon. If you hover over the icon, you see a message such as "Internet access."

- Windows 8.1 or earlier versions:

1. NCSI sends a DNS request to resolve the address of the `www.msftncsi.com` FQDN.
2. If NCSI receives a valid response from a DNS server, NCSI sends a plain HTTP GET request to `http://www.msftncsi.com`/ncsi.txt.
3. If NCSI successfully downloads the text file, it makes sure that the file contains Microsoft NCSI.
4. NCSI sends another DNS request to resolve the address of the `dns.msftncsi.com` FQDN.
    - If any of these requests fails, the network alert appears in the Task Bar (as described in Symptoms). If you hover over the icon, you see a message such as "No connectivity" or "Limited Internet access" (depending on which requests failed).
    - If all of these requests succeed, the Task Bar shows the usual network icon. If you hover over the icon, you see a message such as "Internet access."

NCSI and the NLA service combine these responses with other information to build a profile of the network connection, or identify its existing profile. The network connection profile provides the information that Windows needs to configure the appropriate Windows Firewall profile:

- For Active Directory-authenticated networks: Firewall domain profile.
- For networks that the user has marked as "private": Firewall private profile.
- For networks that the user has marked as "public": Public firewall profile.

> ⓘ **Note**
>
> You can use Group Policy to restrict the active probe process, and you can substitute a different website as a target (although this substitution is not a recommended solution). For more information, see the following resources:
>
> - **Manage connections from Windows operating system components to Microsoft services: 14. Network Connectivity Status Indicator**
> - **Policy CSP - Connectivity: Connectivity/DisallowNetworkConnectivityActiveTests**

Authentication and the automatic sign-in page

If the network requires credentials, Windows opens the default browser (such as Internet Explorer or Edge). If the network has a sign-in page, that page appears in the browser.

This behavior was introduced to improve the Windows user experience. In earlier versions of Windows, when you connect to a network that requires you to authenticate, the browser window does not open automatically. You may see a message that states that you must take further action in order to connect fully to the network. To complete the connection, you must click the message to open a browser window (or manually open a browser window) and enter a user name and password.

Because the network does not allow internet access without credentials, the network alert appears in the Task Bar.

NCSI passive monitoring, the MSN Portal page, and the network status alert

In addition to the active probes that this article describes, NCSI monitors the network activity of other applications on the computer. This passive monitoring process continues even if the active probe process fails. NCSI adjusts its network status determination based on whether other applications can make successful TCP connections. If a network alert appears because of a failed active probe, it disappears when a passive probe succeeds.

> **Note**
>
> The NCSI passive monitoring process does not transfer any information to or from your computer, and does not read any of the information that other applications transfer.

In some cases, such as when you connect to a network that uses a proxy server to connect to the internet or when network restrictions prevent NCSI from completing its active probe process, Windows opens the MSN Portal page in the default browser. If you analyze a network trace on the computer, it shows an HTTP connection to `http://www.msftconnecttest.com/redirect` that is followed by a connection to the MSN Portal. Windows opens this page for the benefit of the passive probe process. If the page loads, NCSI concludes that the computer has internet access. As the different probes fail and then succeed, the network status alert appears and then disappears.

> **Note**

To prevent the browser window from opening when the computer connects to a network that has a proxy server, you have to configure the network firewall to allow access to the following URLs on port 80:

- *.msftncsi.com
- *.msftconnecttest.com

For more information, see **KB 2778122, Using authenticated proxy servers together with Windows 8**

Workaround

You can disable the NCSI active or passive probes by using the registry or Group Policy Objects (GPOs).

⊗ Caution

Microsoft does not recommend disabling the NCSI probes. Several operating system components and applications rely on NCSI. For example, if NCSI does not function correctly, Microsoft Outlook may not be able to connect to a mail server, or Windows may not be able to download updates even if the computer is connected to the internet.

To use the registry to disable NCSI active probes, configure one of the following registry keys.

ⓘ Important

Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, back up the registry for restoration in case problems occur.

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet\EnableActiveProbing`
  - Key Type: DWORD
  - Value: Decimal 0 (False)
- `HKLM\Software\Policies\Microsoft\Windows\NetworkConnectivityStatusIndicator\NoActiveProbe`
  - Key Type: DWORD

- Value: Decimal 1 (True)

> ⓘ **Note**
>
> In the default registry configuration, this registry entry does not exist. You must create it.

To use the registry to disable NCSI passive probes, create the following registry key.

- `HKLM\Software\Policies\Microsoft\Windows\NetworkConnectivityStatusIndicator\DisablePassivePolling`
  - Key Type: DWORD
  - Value: Decimal 1 (True)

> ⓘ **Note**
>
> In the default registry configuration, this registry entry does not exist. You must create it.

To use Group Policy to disable NCSI active probes, configure the following GPO:

- **Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Network Connectivity Status Indicator active tests**
  - Value: Enabled

To use Group Policy to disable NCSI passive probes, configure the following GPO:

- **Computer Configuration\Administrative Templates\Network\Network Connectivity Status Indicator\Specify passive polling**.
  - Value: Enabled

Network gets disconnected for several seconds if the computer isn't used after you sign in to Windows 10

Article • 11/22/2021 • 2 minutes to read

Applies to: Windows 10

Symptoms

When you sign in to a computer running Windows 10 and leave it unused for more than 10 minutes, the network gets disconnected for several seconds.

Applications and services that communicate with the computer through LAN will get disconnected from the computer during that period.

> **Note**
>
> This is a common scenario in **Windows 10 IoT**.

Cause

The Logon pre-scheduled task starts the ProvTool.exe file. This file processes provisioning packages on the system. The ndisuio.sys driver is loaded when the ProvTool.exe starts the DMWapPushService service for the process. When the ndisuio.sys driver binds to the network, the existing connection is interrupted and resumes after a few seconds.

Resolution

Method1: Change the loading time of the ndisuio.sys driver

Here's how to change the loading time of ndisuio.sys driver:

1. Open **Registry Editor**.
2. Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Ndisuio`.

3. Double-click **Start** and change the value data to **1**.

> ⓘ **Note**
>
> The value data **1** represents starting the driver when the system starts.

4. Close **Registry Editor**.

5. Restart the system.

Method 2: Change the start timing of the DMWapPushSvc service

Here's how to change the start timing of the DMWapPushSvc service:

1. Open **Registry Editor**.

2. Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmwappushservice`.

3. Double-click **Start** and change the value data to **2**.

> ⓘ **Note**
>
> The value data **2** represents setting the service to start automatically.

4. Close **Registry Editor**.

5. Restart the system.

Port Scanning Prevention Filter behavior in Windows

Article • 09/23/2021 • 2 minutes to read

This article describes the functionality of the Port Scanning Prevention Filter in Windows Server 2008 and later versions of Windows. It also includes a workaround for the by-design behavior that generates lots of disk I/O when there's activity in the wfpdiag.etl log.

Applies to: Windows Server 2012 R2
Original KB number: 3044882

Symptoms

Consider the following scenario:

- You have a custom networking application installed on your server.
- The application captures lots of traffic on the wire.
- The server may be using a DHCP-assigned IP address.

In this scenario, a large volume of disk I/O may be generated when writes are made to the C:\Windows\System32\wfp\wfpdiag.etl log.

Cause

This behavior is by design. When the Port Scanning Prevention Filter is triggered, this typically means that there's no process listening on the port. (For security reasons, WFP blocks process listening.) When a connection is tried on a port where there's no listener, WFP recognizes the packet as if it was coming from a port scanner and therefore silently drops the connection.

If there had been a listener, and the communication was instead blocked because of either malformed packets or authentication, the dropped event would be listed as "DROP" (not silent), and WFP logging would indicate a different filter ID and name.

This filter is built in to the Windows Firewall and Advanced Security (WFAS). It's included in Windows Vista, Windows Server 2008, and later versions of Windows.

Workaround

To work around this issue, disable WFP logging by using one of the following methods:

- Disable WFP logging by running the following Netsh command from an elevated command prompt:

  ```
  Console

  netsh wfp set options netevents=off
  ```

- Disable WFP logging in the registry. To do this, follow these steps:

  1. Start Registry Editor.
  2. Locate the following registry subkey:
     `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BFE\Parameters\Policy\Options`
  3. Right-click the subkey, click **New**, and then create a DWORD (32-bit) registry value.
  4. Type *CollectNetEvents* as the registry value name.
  5. Leave the value data as 0.
  6. Restart the server.

> ⓘ **Note**
>
> By disabling WFP logging, this only stops the logging of WFP activity in wfpdiag.etl. The Port Scanning Prevention Filter continues to work normally.

More information

For more information, see Stealth mode in Windows Firewall with Advanced Security.

Set up your small business network

Article • 03/24/2022 • 75 minutes to read

This article walks you through the steps of evaluating, preparing, and setting up your small business network. The article is for IT Pros who help set up your small business network.

Applies to: Windows 10 - all editions, Windows Server 2012 R2 *Original KB number:* 10064

Evaluate network types

Many small businesses use a network to share access to the Internet, printers, and files from one computer to another. While having a network almost surely benefits your business, you need to decide which kind of network is the best option for your business depending on its unique and specific needs. The choices you have are wired, wireless, and hybrid networks. When you select a network for your business, you should consider two main points - the location of your devices and how fast you want your network to be. Although costs are similar between the different types, prices will vary according to the network speed that you select.

The following sections describe the different network options available.

Wired networks

Wired or Ethernet networks can transfer data from 10 Mbps to 1000 Mbps, depending on the type of cables you use. Gigabit Ethernet provides the fastest transfer rate at up to 1 gigabit per second (1000 Mbps).

Advantages

- Ethernet networks are highly secure and fast.
- Ethernet networks are safer than wireless networks because they're fully contained.
- Ethernet networks aren't affected by interference of objects or walls.

Drawbacks

- You must run Ethernet cables between each device and a hub, switch, or router. It can be time-consuming and difficult when devices are in different rooms.
- The hardware is more expensive.

Hardware requirements

Hardware	How many
Ethernet network adapter An adapter connects devices to a network so that they can communicate. You can connect a network adapter to a USB port with either Ethernet cables or USB cables, depending on the type of adapter. You can also install a network adapter inside a device.	One for each device on your network. Desktop computers usually have these adapters built in.
Ethernet hub or switch A hub passes data from one device to another. Because the hub can't identify the data source as coming from the Internet or another device, it sends the information to all connected devices, including the one that sent it. A switch works similar to a hub. But a switch can also identify the intended destination of the information so that only the intended devices receive it. A switch costs a bit more than a hub, but has faster speed.	One. A 10/100/1000 hub or switch is best and should have enough ports to accommodate all the devices on your network.
Ethernet router (only needed if you want to connect more than two devices that share an Internet connection) A router helps you share a single Internet connection among several devices. You don't require a router to set up a wired network, but you should use one if you want multiple devices to share an Internet connection.	One. You might need an extra hub or switch if your router doesn't have enough ports for all of your devices.
Modem Devices use modems to send and receive information over telephone or cable lines. You need a modem if you want to connect to the Internet.	One.
Ethernet cables Network cables connect devices to one another and to other related hardware, such as hubs, routers, and external network adapters.	One for each device that needs to connect to the network hub or switch. 10/100/1000 Cat 6 cables are best, but not required.

Wireless networks

Wireless networks can transfer data anywhere from 10-600 megabytes per second (Mbps) depending on the type of wireless standard that your modem uses.

Advantages

- You can easily move devices because there are no cables.
- Wireless networks are cheaper to install than wired networks.

- You can often improve the wireless signal by using a wireless repeater. Wireless repeaters pick up a signal, and if the signal has degraded, the repeater can rebroadcast it again at full strength.

Drawbacks

- Wireless technology is often slower than wired technologies.
- Wireless technology can be affected by interference from walls, large metal objects, and pipes. Also, many cordless phones and microwave ovens can interfere with wireless networks when in use.
- Wireless networks are frequently about half as fast as their rated speed.

Hardware requirements

Hardware	How many
Wireless network adapter An adapter connects devices to a network so that they can communicate.	One for each device on your network. Portable devices usually have them built in.
Wireless router A router helps you share a single Internet connection among several devices. You don't require a router to set up a wired network, but you should use one if you want multiple devices to share an Internet connection.	One.

If your device has built-in wireless capabilities, then you don't need a wireless network adapter.

Hybrid networks

Hybrid networks use a combination of wireless and wired networks and offer the best of both network types so that you can use faster wired desktops and portable wireless mobile devices, such as laptops, tablets and smartphones. A hybrid network relies on special hybrid routers, hubs, switches, and Ethernet cables to connect wired and wireless devices. A hybrid router does two things - broadcasts a wireless signal and provides wired access ports. It's most commonly referred to as a wireless or Wi-Fi router with Ethernet ports or "LAN ports".

A hybrid wired/wireless network seems to offer the best of both worlds in speed, mobility, affordability and security. If users need maximum Internet and file-sharing speed, they can plug into the network with an Ethernet cable. If they need to share a

streaming video in the office hallway, they can access the network wirelessly. With the right planning, an organization can save money on CAT5/CAT6 cables and routers by maximizing the reach of the wireless network. With the right encryption and password management in place, the wireless portion of the network can be as secure as the wired.

Hardware	How many
Network adapter An adapter connects devices to a network so that they can communicate.	One for each device on your network. Both desktops and portable devices usually have these adapters built in.
hybrid router A router helps you share a single Internet connection among several devices. You don't require a router to set up a wired network, but you should use one if you want multiple devices to share an Internet connection.	At least one. If you need to connect more than four wired devices, add an extra wired router.
Ethernet cables Network cables connect devices to one another and to other related hardware, such as hubs, routers, and external network adapters.	One for each device connected to the network hub or switch. 10/100/1000 Cat 6 cables are best, but not required.

Install a wired network

Wired networks are faster, more secure, and reliable than wireless networks. They also reduce the chance of outside interference. At the same time, they require a bit more work to set up and the hardware is more expensive.

> ⓘ **Note**
>
> If your small business has lots of floor space, such as a manufacturing facility, you may experience signal degradation if there are very long cables between devices. You can often improve the signal by using an Ethernet repeater to strengthen the signal. To begin, follow the procedure for the version of Windows running on the device that you want to connect to your network. All of your devices don't need to run the same version of Windows to be a part of your business network.

Connect the cables

To begin, run an Ethernet cable from the router or hub to each device that you want to connect to the network.

Install the network adapters

Windows can automatically detect and install the correct network adapter software for you.

To check whether your device has a network adapter, follow the instructions.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Type *device manager* in the Search box.
4. Tap or click **Settings**.
5. Tap or click **Device Manager** on the left side of your screen.
6. To see a list of installed network adapters, expand Network adapter(s).

Set up your router

If your router displays the Windows logo or the phrase Compatible with Windows, you can set it up automatically using the latest version of Windows Connect Now (WCN). Otherwise, most routers come with instructions and a setup CD that will help you set them up.

If you have a combined modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the wide area network (WAN) port of the device and then plug the other end into the wall jack. The WAN port should be labeled "WAN." (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the local area network (LAN) port on the device and the other end into the networking port of the device that you want to connect to the Internet. The LAN port should be labeled "LAN."
4. Start (or restart) the device.

Connect your router to the Internet

To connect your router to the Internet, follow the instructions.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Tap or click the down arrow next to **Everywhere** above the Search box, and tap or click **Settings**.
4. Type *network and sharing center* in the Search box.

5. Tap or click **Network and Sharing Center** from the search result.
6. Tap or click Set up a new **connection or network**.
7. Tap or click **Connect to the Internet**.
8. Tap or click **Next**.

If your home or office is wired for Ethernet, set up the devices in rooms that have Ethernet jacks, and then plug them directly into the Ethernet jacks.

Set up a separate modem to attach to a router

If you purchased a separate modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the modem and the other end into the wall jack. (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the modem and the other end into the wide area network (WAN) port on the router.
4. Plug the router into an electrical outlet.
5. Plug one end of an Ethernet cable into the local area network (LAN) port on the router and the other end into the networking port on the device that you want to connect to the Internet.
6. Start or restart the device.

Connect the modem to the Internet

Follow the instructions to Connect the modem to the Internet.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Tap or click the down arrow next to **Everywhere** above the Search box, and tap or click **Settings**.
4. Type *network and sharing center* in the Search box.
5. Tap or click **Network and Sharing Center** from the search result.
6. Tap or click **Set up a new connection or network**.
7. Tap or click **Connect to the Internet**.
8. Tap or click **Next**.

Set up a firewall

A firewall is hardware or software that helps control the spread of malicious software on your network and helps to protect your devices when you use the Internet.

Don't turn off Windows Firewall unless you have another firewall turned on. Turning off Windows Firewall might make your device and network vulnerable to damage from hackers. To set up a firewall, follow the instructions:

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Type *firewall* in the Search box.
4. Tap or click **Settings**.
5. Tap or click **Windows Firewall** on the left side of your screen.
6. In the left pane, tap or click **Turn Windows Firewall on or off**.
7. Tap or click **Turn on Windows Firewall** under each type of network that you want to help protect, and then tap or click **OK**.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Enable file and printer sharing with a firewall

Windows Firewall automatically opens the correct ports for file and printer sharing when you share content or turn on network discovery. If you're using another firewall, you must open these ports yourself so that your device can find other devices that have files or printers that you want to share.

To find other devices running Windows 8, Windows 7, or Windows Vista, open these ports:

- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

To find other devices running earlier versions of Windows, and to use file and printer sharing on any version of Windows, open these ports:

- UDP 137
- UDP 138
- TCP 139

- TCP 445
- UDP 5355

To find network devices, open these ports:

- UDP 1900
- TCP 2869
- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

Connect devices to the network

If the devices running Windows 7 are connected to either a hub or a switch using a cable, then they're already on the network, and ready to use.

If you had to change the workgroup name, you're prompted to restart your device. Restart the device, and then continue with the following steps.

1. Click **Start**.
2. Click **My Network Places**.
3. In the left pane, under **Network Tasks**, click **View workgroup computers**.
4. Select the device from the list that appears and click **Connect**.

Connect the cables

To begin, run an Ethernet cable from the router or hub to each device that you want to connect to the network.

Install the network adapters

Windows can automatically detect and install the correct network adapter software for you. To check whether your device has a network adapter, follow the instructions.

1. Right-click **Computer**.
2. Click **Properties**.
3. Click **Device Manager** on the left pane.
4. To see a list of installed network adapters, expand Network adapter(s).

Set up your router

If your router displays the Windows logo or the phrase Compatible with Windows, you can set it up automatically using the latest version of Windows Connect Now (WCN). Otherwise, most routers come with instructions and a setup CD that will help you set them up.

If you have a combined modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the wide area network (WAN) port of the device and then plug the other end into the wall jack. The WAN port should be labeled "WAN." (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the local area network (LAN) port on the device and the other end into the networking port of the device that you want to connect to the Internet. The LAN port should be labeled "LAN."
4. Start (or restart) the device.

Connect your router to the Internet

To connect your router to the Internet, follow the instructions.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. Click **Set up a connection or network**.
6. Click **Connect to the Internet**.
7. Follow the instructions in the wizard.

If your home or office is wired for Ethernet, set up the devices in rooms that have Ethernet jacks, and then plug them directly into the Ethernet jacks.

Set up a separate modem to attach to a router

If you purchased a separate modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the modem and the other end into the wall jack. (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the modem and the other end into the wide area network (WAN) port on the router.
4. Plug the router into an electrical outlet.

5. Plug one end of an Ethernet cable into the local area network (LAN) port on the router and the other end into the networking port on the device that you want to connect to the Internet.
6. Start or restart the device.

Connect the modem to the Internet

Follow the instructions to connect the modem to the Internet.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. Click **Set up a connection or network**.
6. Click **Connect to the Internet**.
7. Follow the instructions in the wizard.

Set up a firewall

A firewall is hardware or software that helps control the spread of malicious software on your network and helps to protect your devices when you use the Internet.

Don't turn off Windows Firewall unless you have another firewall turned on. Turning off Windows Firewall might make your device and network vulnerable to damage from hackers.

To set up a firewall, follow the instructions:

1. Click **Start**.
2. Click **Control Panel**.
3. Type firewall in the **Search** box.
4. Click **Windows Firewall**.
5. In the left pane, click **Turn Windows Firewall on or off**.
6. Tap or click **Turn on Windows Firewall** under each type of network that you want to help protect, and then tap or click **OK**.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Enable file and printer sharing with a firewall

Windows Firewall automatically opens the correct ports for file and printer sharing when you share content or turn on network discovery. If you're using another firewall, you must open these ports yourself so that your device can find other devices that have files or printers that you want to share.

To find other devices running Windows 8, Windows 7, or Windows Vista, open these ports:

- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

To find other devices running earlier versions of Windows, and to use file and printer sharing on any version of Windows, open these ports:

- UDP 137
- UDP 138
- TCP 139
- TCP 445
- UDP 5355

To find network devices, open these ports:

- UDP 1900
- TCP 2869
- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

To make HomeGroup work between devices running Windows 7, open these ports:

- UDP 137
- UDP 138
- TCP 139
- T CP 445
- UDP 1900
- TCP 2869
- UDP 3540

- TCP 3587
- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

Connect devices to the network

If the devices running Windows Vista are connected to either a hub or a switch using a cable, then they're already on the network, and ready to use.

If you had to change the workgroup name, you're prompted to restart your device. Restart the device, and then continue with the following steps.

1. Click **Start**.
2. Click **My Network Places**.
3. In the left pane, under **Network Tasks**, click **View workgroup computers**.
4. Select the device from the list that appears and click **Connect**.

Connect the cables

To begin, run an Ethernet cable from the router or hub to each device that you want to connect to the network.

Install the network adapters

Windows can automatically detect and install the correct network adapter software for you. To check whether your device has a network adapter, follow the instructions.

1. Right-click **Computer**.
2. Click **Properties**.
3. Click **Device Manager** on the left pane.
4. To see a list of installed network adapters, expand Network adapter(s).

Set up your router

If your router displays the Windows logo or the phrase Compatible with Windows, you can set it up automatically using the latest version of Windows Connect Now (WCN). Otherwise, most routers come with instructions and a setup CD that will help you set them up.

If you have a combined modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the wide area network (WAN) port of the device and then plug the other end into the wall jack. The WAN port should be labeled "WAN." (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the local area network (LAN) port on the device and the other end into the networking port of the device that you want to connect to the Internet. The LAN port should be labeled "LAN."
4. Start (or restart) the device.

Connect your router to the Internet

To connect your router to the Internet, follow the instructions.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. Click **Set up a connection or network**.
6. Click **Connect to the Internet**.
7. Follow the instructions in the wizard.

If your home or office is wired for Ethernet, set up the devices in rooms that have Ethernet jacks, and then plug them directly into the Ethernet jacks.

Set up a separate modem to attach to a router

If you purchased a separate modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the modem and the other end into the wall jack. (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the modem and the other end into the wide area network (WAN) port on the router.
4. Plug the router into an electrical outlet.
5. Plug one end of an Ethernet cable into the local area network (LAN) port on the router and the other end into the networking port on the device that you want to connect to the Internet.
6. Start or restart the device.

Connect the modem to the Internet

Follow the instructions to connect the modem to the Internet.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. Click **Set up a connection or network**.
6. Click **Connect to the Internet**.
7. Follow the instructions in the wizard.

Set up a firewall

A firewall is hardware or software that helps control the spread of malicious software on your network and helps to protect your devices when you use the Internet.

Don't turn off Windows Firewall unless you have another firewall turned on. Turning off Windows Firewall might make your device and network vulnerable to damage from hackers.

To set up a firewall, follow the instructions:

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Security**.
4. Click **Windows Firewall**.
5. Click **Turn Windows Firewall on or off**.
6. Click **On** (recommended), and then click **OK**.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Enable file and printer sharing with a firewall

Windows Firewall automatically opens the correct ports for file and printer sharing when you share content or turn on network discovery. If you're using another firewall, you must open these ports yourself so that your device can find other devices that have files or printers that you want to share.

To find other devices running Windows 8, Windows 7, or Windows Vista, open these ports:

- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

To find other devices running earlier versions of Windows, and to use file and printer sharing on any version of Windows, open these ports:

- UDP 137
- UDP 138
- TCP 139
- TCP 445
- UDP 5355

To find network devices, open these ports:

- UDP 1900
- TCP 2869
- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

Connect devices to the network

If the devices running Windows Vista are connected to either a hub or a switch using a cable, then they're already on the network, and ready to use.

If you had to change the workgroup name, you're prompted to restart your device. Restart the device, and then continue with the following steps.

1. Click **Start**.
2. Click **My Network Places**.
3. In the left pane, under **Network Tasks**, click **View workgroup computers**.
4. Select the device from the list that appears and click **Connect**.

Connect the cables

To begin, run an Ethernet cable from the router or hub to each device that you want to connect to the network.

Install the network adapters

Windows can automatically detect and install the correct network adapter software for you.

To check whether your device has a network adapter, follow the instructions.

1. Click **Start**.
2. Right-click **My Computer**.
3. Click **Properties**.
4. Under **Hardware** tab, click **Device Manager**.
5. To see a list of installed network adapters, expand Network adapter(s).

Set up your router

If your router displays the Windows logo or the phrase Compatible with Windows, you can set it up automatically using the latest version of Windows Connect Now (WCN). Otherwise, most routers come with instructions and a setup CD that will help you set them up.

If you have a combined modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the wide area network (WAN) port of the device and then plug the other end into the wall jack. The WAN port should be labeled "WAN." (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the local area network (LAN) port on the device and the other end into the networking port of the device that you want to connect to the Internet. The LAN port should be labeled "LAN."
4. Start (or restart) the device.

Connect your router to the Internet

To connect your router to the Internet, follow the instructions.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet Connections**.
4. Click **Set up or change your Internet connection**.
5. Click **Setup**.
6. Follow the instructions in the **New Connection Wizard** to connect to the Internet.

Building already wired for Ethernet

If your home or office is wired for Ethernet, set up the devices in rooms that have Ethernet jacks, and then plug them directly into the Ethernet jacks.

Set up a separate modem to attach to a router

If you purchased a separate modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the modem and the other end into the wall jack. (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the modem and the other end into the wide area network (WAN) port on the router.
4. Plug the router into an electrical outlet.
5. Plug one end of an Ethernet cable into the local area network (LAN) port on the router and the other end into the networking port on the device that you want to connect to the Internet.
6. Start or restart the device.

Connect the modem to the Internet

Follow the instructions to connect the modem to the Internet.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet Connections**.
4. Click **Set up or change your Internet connection**.
5. Click **Setup**.
6. Follow the instructions in the **New Connection Wizard** to connect to the Internet.

Set up a firewall

A firewall is hardware or software that helps control the spread of malicious software on your network and helps to protect your devices when you use the Internet.

Don't turn off Windows Firewall unless you have another firewall turned on. Turning off Windows Firewall might make your device and network vulnerable to damage from hackers.

To Set up a firewall, follow the instructions:

1. Click **Start**.
2. Click **Run**.

3. Type **Firewall.cpl**, and click **OK**.
4. On the General tab, click **On** (recommended).
5. Click **OK**.

Enable file and printer sharing with a firewall

Windows Firewall automatically opens the correct ports for file and printer sharing when you share content or turn on network discovery. If you're using another firewall, you must open these ports yourself so that your device can find other devices that have files or printers that you want to share.

To find other devices running Windows XP or earlier versions of Windows, and to use file and printer sharing on any version of Windows, open these ports:

- UDP 137
- UDP 138
- TCP 139
- TCP 445
- UDP 5355

To find network devices, open these ports:

- UDP 1900
- TCP 2869
- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

Connect devices to the network

If you have devices running Windows XP, you may need to do a little more work to add those devices.

To add a wired (Ethernet) device that is running Windows XP

1. Plug the device into a hub, switch, or router and turn it on. If your home has Ethernet wiring and you have a jack in the room where the device is, you can plug the device into the Ethernet jack instead.
2. Log on to the device as an administrator.
3. Click **Start**, right-click **My Computer**, and then click **Properties**.
4. Click the **Computer Name** tab and then click **Change**.

5. If the workgroup name isn't WORKGROUP, change the name to WORKGROUP and click **OK**.

If you had to change the workgroup name, you're prompted to restart your device. Restart the device, and then continue with the following steps.

1. Click **Start**.
2. Click **My Network Places**.
3. In the left pane, under **Network Tasks**, click **View workgroup computers**.
4. Select the device from the list that appears and click **Connect**.

Install a wireless network

Now that you've decided to invest in a wireless network for your business, you have to select a network standard and set up your network. Wireless networks (WLANs) don't require much in the way of network infrastructure. Many small business owners select wireless networking because it's flexible, inexpensive, and easy to install and maintain. You can use a wireless network to share Internet access, files, printers, file servers, and other devices in your office. Once you have the network set up, you can enable sharing, set permissions, and add printers and other devices.

To begin, follow the procedure for the version of Windows running on the device that you want to connect to your network. All of your devices don't need to run the same version of Windows to be a part of your business network.

Select a wireless network standard

The most common wireless network standards are 802.11b, 802.11g, 802.11a, and 802.11n. Prices vary for each standard as do data transfer rates. Typically the faster the data transfer rate, the more you pay. In general, data transfer rates for each standard work as follows:

1. 802.11b —11 Megabytes per second (Mbps)
2. 802.11g — 54 Mbps
3. 802.11a — 54 Mbps
4. 802.11n — 300-600 Mbps

> **Note**
>
> The transfer times listed are under ideal conditions. They aren't necessarily achievable under typical circumstances because of differences in hardware, web servers, network traffic, and other factors.

Set up your wireless router

A wireless router sends information between your network and the Internet by using radio signals instead of wires. You should use a router that supports faster wireless signals, such as 802.11g or 802.11n.

For the best results, put your wireless router, wireless modem router (a DSL or cable modem with a built-in wireless router), or wireless access point (WAP) in a central location in your office. If your router is on the first floor and your devices are on the second floor, put the router high on a shelf on the first floor.

> ⓘ **Note**
>
> Metal objects, walls, and floors can interfere with your router's wireless signals.

Set up your modem and Internet connection

If your ISP didn't set up your modem, follow the instructions that came with your modem to connect it to your device and the Internet. If you're using a Digital Subscriber Line (DSL), connect your modem to a telephone jack. If you're using cable, connect your modem to a cable jack.

Set up a modem and router

To set up two pieces of hardware, a modem and a router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the modem and the other end into the wall jack. (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the modem and the other end into the wide area network (WAN) port on the router.
4. Plug the router into an electrical outlet.
5. Start (or restart) the device.
6. Now follow the instructions in the section below to complete the modem and router setup.

> ⓘ **Note**

> Protect your router by changing the default user name and password. Most router manufacturers have a default user name and password on the router in addition to a default network name. Someone could use this information to access your router without your knowledge. Check the information that was included with your device for instructions.

Set up a combined modem and router

If you have a combined modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the wide area network (WAN) port of the device and the other into the wall jack. The WAN port should be labeled WAN. (DSL users shouldn't use a DSL filter on the phone line.)
3. Once completed, restart your device.

Complete the modem and router setup

To complete the modem and router setup, follow the instructions to complete set up.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Type *network and sharing center* in the Search box.
4. Tap or click **Settings**.
5. Tap or click **Network and Sharing Center** on the left side of your screen.
6. Tap or click **Set up a new connection or network**.
7. Tap or click **Connect to the Internet**.
8. Tap or click **Next**.

A network adapter connects your device to a network

To connect to a wireless network, your device must have a wireless network adapter. Make sure that you get the same type of adapters as your wireless router. The type of adapter is marked on the package with a letter, such as G or A.

To check whether your device has a wireless network adapter, follow the instructions.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.

3. Type **Control panel** in the Search box.
4. Tap or click **Apps**.
5. Tap or click **Control Panel** on the left side of your screen.
6. Type Device Manager in the Search Control Panel box.
7. Tap or click **Device Manager**.
8. Double-tap or double-click **Network adapters**.
9. Look for a network adapter that includes "wireless" in the name.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Set up a security key for your network

Every wireless network has a network security key to help protect it from unauthorized access.

To set up a network security key, follow the instructions.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Settings**.
3. Tap or click **Network** icon.
4. Select your wireless network from the list that appears and tap or click **Connect**.

> ⓘ **Note**
>
> Whenever possible, you should connect to a security-enabled wireless network. If you do connect to a network that's not secure, someone with the right tools can see everything that you do, including the websites you visit, the documents you work on, and the user names and passwords that you use.

5. Select one of the following options:

    - If your router supports Windows Connect Now (WCN) or Wi-Fi Protected Setup (WPS), and there's a push button on the router, push the button and wait a few seconds while the router automatically adds the device to the network. In this instance, you don't need to enter a security key or passphrase.
    - Enter the security key or passphrase if prompted and tap or click **OK**.

Set up a firewall

A firewall is hardware or software that helps protect your device from hackers or malicious software.

Running a firewall on each device on your network can help control the spread of malicious software on your network and help protect your devices when you use the Internet.

Don't turn off Windows Firewall unless you have another firewall turned on. Turning off Windows Firewall might make your device and network vulnerable to damage from hackers.

To set up a firewall, follow the instructions:

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Type *firewall* in the Search box.
4. Tap or click **Settings**.
5. Tap or click **Windows Firewall** on the left side of your screen.
6. In the left pane, tap or click **Turn Windows Firewall on or off**.
7. Tap or click **Turn on Windows Firewall** under each type of network that you want to help protect, and then tap or click **OK**.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Enable file and printer sharing with a firewall

Windows Firewall automatically opens the correct ports for file and printer sharing when you share content or turn on network discovery. If you're using another firewall, you must open these ports yourself so that your device can find other devices that have files or printers that you want to share.

To find other devices running Windows 8, Windows 7, or Windows Vista, open these ports:

- UDP 3702
- UDP 5355
- TCP 5357

- TCP 5358

To find other devices running earlier versions of Windows, and to use file and printer sharing on any version of Windows, open these ports:

- UDP 137
- UDP 138
- TCP 139
- TCP 445
- UDP 5355

To find network devices, open these ports:

- UDP 1900
- TCP 2869
- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

Save your wireless network settings to a USB flash drive

Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Settings**.
3. Tap or click **Network** icon.
4. Right-click the network and then click **View connection properties**.
5. Under the **Connection** tab, click **Copy this network profile to a USB flash drive**.
6. Select the USB device and click **Next**.
7. Follow the instructions in the wizard and then click **Close**.

Use a USB flash drive to connect to the network

If you want to use a USB flash drive to copy network settings to your device instead of typing a security key or passphrase, follow these steps:

1. Log on to the device that you want to add to the network.
2. Plug the USB flash drive that contains the network settings into a USB port on the device. For a device running Windows 8.1 and Windows 8, tap or click the

notification about the USB flash drive when it displays. In the USB flash drive dialog box, tap or click **Wireless Network Setup Wizard**.

Connect devices to the network

To connect a device to your network, follow the instructions.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Settings**.
3. Tap or click **Network** icon.
4. Select the wireless network from the list that appears and tap or click **Connect**.
5. Enter the security key if prompted and tap or click **OK**.

Select a wireless network standard

The most common wireless network standards are 802.11b, 802.11g, 802.11a, and 802.11n. Prices vary for each standard as do data transfer rates. Typically the faster the data transfer rate, the more you pay. In general, data transfer rates for each standard work as follows:

1. 802.11b —11 Megabytes per second (Mbps)
2. 802.11g — 54 Mbps
3. 802.11a — 54 Mbps
4. 802.11n — 300-600 Mbps

> ⓘ **Note**
>
> The transfer times listed are under ideal conditions. They aren't necessarily achievable under typical circumstances because of differences in hardware, web servers, network traffic, and other factors.

Set up your wireless router

A wireless router sends information between your network and the Internet by using radio signals instead of wires. You should use a router that supports faster wireless signals, such as 802.11g or 802.11n.

For the best results, put your wireless router, wireless modem router (a DSL or cable modem with a built-in wireless router), or wireless access point (WAP) in a central

location in your office. If your router is on the first floor and your devices are on the second floor, put the router high on a shelf on the first floor.

> ⓘ **Note**
>
> Metal objects, walls, and floors can interfere with your router's wireless signals.

Set up your modem and Internet connection

If your ISP didn't set up your modem, follow the instructions that came with your modem to connect it to your device and the Internet. If you're using a Digital Subscriber Line (DSL), connect your modem to a telephone jack. If you're using cable, connect your modem to a cable jack.

Set up a modem and router

To set up two pieces of hardware, a modem and a router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the modem and the other end into the wall jack. (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the modem and the other end into the wide area network (WAN) port on the router.
4. Plug the router into an electrical outlet.
5. Start (or restart) the device.
6. Now follow the instructions in the section below to complete the modem and router setup.

   > ⓘ **Note**
   >
   > Protect your router by changing the default user name and password. Most router manufacturers have a default user name and password on the router in addition to a default network name. Someone could use this information to access your router without your knowledge. Check the information that was included with your device for instructions.

Set up a combined modem and router

If you have a combined modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the wide area network (WAN) port of the device and the other into the wall jack. The WAN port should be labeled **WAN**. (DSL users shouldn't use a DSL filter on the phone line.)
3. Once completed, restart your device.

Complete the modem and router setup

To complete the modem and router setup, follow the instructions:

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. Click **Set up a connection or network**.
6. Click **Connect to the Internet**.
7. Follow the instructions in the wizard.

Set up your wireless network adapters

To check whether your device has a wireless network adapter, follow the instructions.

1. Click **Start**.
2. Type network in the Search box.
3. Click **Device Manager**.
4. Next to **Network adapters**, click the plus sign (+).
5. Look for a network adapter that includes "wireless" in the name.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Set up a firewall

A firewall is hardware or software that helps control the spread of malicious software on your network and helps to protect your devices when you use the Internet.

Don't turn off Windows Firewall unless you have another firewall turned on. Turning off Windows Firewall might make your device and network vulnerable to damage from hackers.

To set up a firewall, follow the instructions:

1. Click **Start**.
2. Click **Control Panel**.
3. Type firewall in the Search box.
4. Click **Windows Firewall**.
5. In the left pane, click **Turn Windows Firewall on or off**.
6. Tap or click **Turn on Windows Firewall** under each type of network that you want to help protect and then tap or click **OK**.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Enable file and printer sharing with a firewall

Windows Firewall automatically opens the correct ports for file and printer sharing when you share content or turn on network discovery. If you're using another firewall, you must open these ports yourself so that your device can find other devices that have files or printers that you want to share.

To find other devices running Windows 8, Windows 7, or Windows Vista, open these ports:

- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

To find other devices running earlier versions of Windows, and to use file and printer sharing on any version of Windows, open these ports:

- UDP 137
- UDP 138
- TCP 139
- TCP 445
- UDP 5355

To find network devices, open these ports:

- UDP 1900
- TCP 2869

- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

To make HomeGroup work between devices running Windows 7, open these ports:

- UDP 137
- UDP 138
- TCP 139
- TCP 445
- UDP 1900
- TCP 2869
- UDP 3540
- TCP 3587
- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

Save your wireless network settings to a USB flash drive

1. Right-click the **Network** icon and click **Open Network and sharing Center**.
2. Click **Manage wireless networks**.
3. Right-click the network and click **Properties**.
4. Click **Copy this network profile to a USB flash drive**.
5. Select the USB device and click **Next**.
6. Follow the instructions in the wizard and then click **Close**.

Use a USB flash drive to connect to the network

If you want to use a USB flash drive to copy network settings to your device instead of typing a security key or passphrase, follow these steps:

1. Log on to the device that you want to add to the network.
2. Plug the USB flash drive that contains the network settings into a USB port on the device. For a device running Windows 7, in the **AutoPlay** dialog box, click **Wireless Network Setup Wizard**.

Connect devices to the network

To connect a device to your network, follow the instructions.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. Click **Connect to a network**.
6. Select the wireless network from the list that appears and click **Connect**.
7. Enter the security key if prompted and click **OK**.

Select a wireless network standard

The most common wireless network standards are 802.11b, 802.11g, 802.11a, and 802.11n. Prices vary for each standard as do data transfer rates. Typically the faster the data transfer rate, the more you pay. In general, data transfer rates for each standard work as follows:

1. 802.11b —11 Megabytes per second (Mbps)
2. 802.11g — 54 Mbps
3. 802.11a — 54 Mbps
4. 802.11n — 300-600 Mbps

> **Note**
>
> The transfer times listed are under ideal conditions. They aren't necessarily achievable under typical circumstances because of differences in hardware, web servers, network traffic, and other factors.

Set up your wireless router

A wireless router sends information between your network and the Internet by using radio signals instead of wires. You should use a router that supports faster wireless signals, such as 802.11g or 802.11n.

For the best results, put your wireless router, wireless modem router (a DSL or cable modem with a built-in wireless router), or wireless access point (WAP) in a central location in your office. If your router is on the first floor and your devices are on the second floor, put the router high on a shelf on the first floor.

> **Note**

Metal objects, walls, and floors can interfere with your router's wireless signals.

Set up your modem and Internet connection

If your ISP didn't set up your modem, follow the instructions that came with your modem to connect it to your device and the Internet. If you're using a Digital Subscriber Line (DSL), connect your modem to a telephone jack. If you're using cable, connect your modem to a cable jack.

Set up a modem and router

To set up two pieces of hardware, a modem and a router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the modem and the other end into the wall jack. (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the modem and the other end into the wide area network (WAN) port on the router.
4. Plug the router into an electrical outlet.
5. Start (or restart) the device.
6. Now follow the instructions in the section below to complete the modem and router setup.

> ⓘ **Note**
>
> Protect your router by changing the default user name and password. Most router manufacturers have a default user name and password on the router in addition to a default network name. Someone could use this information to access your router without your knowledge. Check the information that was included with your device for instructions.

Set up a combined modem and router

If you have a combined modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the wide area network (WAN) port of the device and the other into the wall jack. The WAN port should be labeled WAN. (DSL users shouldn't use a DSL filter on the phone line.)
3. Once completed, restart your device.

Complete the modem and router setup

To complete the modem and router setup, follow the instructions to complete set up.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. Click **Set up a connection or network**.
6. Click **Connect to the Internet**.
7. Follow the instructions in the wizard.

Set up your wireless network adapters

A network adapter connects your device to a network. To connect to a wireless network, your device must have a wireless network adapter. Make sure that you get the same type of adapters as your wireless router. The type of adapter is marked on the package with a letter, such as G or A.

To check whether your device has a wireless network adapter, follow the instructions.

1. Click **Start**.
2. Type *network* in the Search box.
3. Click **Device Manager**.
4. Next to **Network adapters**, click the plus sign (+).
5. Look for a network adapter that includes "wireless" in the name.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Set up a security key for your network

Every wireless network has a network security key to help protect it from unauthorized access.

To set up a network security key, follow the instructions.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.

5. Click **Set up a connection or network**.
6. Click **Set up a new network**.
7. Click **Next**. The wizard will walk you through the process of creating a network name and security key. If your router supports it, the wizard will default to Wi-Fi Protected Access (WPA or WPA2) security. We recommend that you use WPA2, if possible. WPA2 offers better security than WPA or Wired Equivalent Privacy (WEP) security. With WPA2 or WPA, you can also use a passphrase.

Make sure that you write the security key and keep it in a safe place. If you have a USB flash drive, you can also save your security key to the flash drive by following the instructions in the wizard.

Set up a firewall

A firewall is hardware or software that helps control the spread of malicious software on your network and helps to protect your devices when you use the Internet.

Don't turn off Windows Firewall unless you have another firewall turned on. Turning off Windows Firewall might make your device and network vulnerable to damage from hackers.

To set up a firewall, follow the instructions:

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Security**.
4. Click **Windows Firewall**.
5. Click **Turn Windows Firewall on or off**.
6. Click **On** (recommended), and then click **OK**.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Enable file and printer sharing with a firewall

Windows Firewall automatically opens the correct ports for file and printer sharing when you share content or turn on network discovery. If you're using another firewall, you must open these ports yourself so that your device can find other devices that have files or printers that you want to share.

To find other devices running Windows 8, Windows 7, or Windows Vista, open these ports:

- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

To find other devices running earlier versions of Windows, and to use file and printer sharing on any version of Windows, open these ports:

- UDP 137
- UDP 138
- TCP 139
- TCP 445
- UDP 5355

To find network devices, open these ports:

- UDP 1900
- TCP 2869
- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

Save your wireless network settings to a USB flash drive

1. Right-click the **Network** icon and click **Open Network and sharing Center**.
2. Click **Manage wireless networks**.
3. Right-click the network and click **Properties**.
4. Click **Copy this network profile to a USB flash drive**.
5. Select the USB device and click **Next**.
6. Follow the instructions in the wizard and then click **Close**.

Use a USB flash drive to connect to the network

If you want to use a USB flash drive to copy network settings to your device instead of typing a security key or passphrase, follow these steps:

1. Log on to the device that you want to add to the network.
2. Plug the USB flash drive that contains the network settings into a USB port on the device. For a device running Windows Vista, in the **AutoPlay** dialog box, click

Wireless Network Setup Wizard.

Connect devices to the network

To connect a device to your network, follow the instructions.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. Click **Connect to a network**.
6. Select the wireless network from the list that appears and click **Connect**.
7. Enter the security key if prompted and click **OK**.

> ⓘ **Note**
>
> You can enter in the key or insert a USB flash drive that contains the security key into a USB port on the device.

Select a wireless network standard

The most common wireless network standards are 802.11b, 802.11g, 802.11a, and 802.11n. Prices vary for each standard as do data transfer rates. Typically the faster the data transfer rate, the more you pay. In general, data transfer rates for each standard work as follows:

1. 802.11b —11 Megabytes per second (Mbps)
2. 802.11g — 54 Mbps
3. 802.11a — 54 Mbps
4. 802.11n — 300-600 Mbps

> ⓘ **Note**
>
> The transfer times listed are under ideal conditions. They aren't necessarily achievable under typical circumstances because of differences in hardware, web servers, network traffic, and other factors.

Set up your wireless router

A wireless router sends information between your network and the Internet by using radio signals instead of wires. You should use a router that supports faster wireless signals, such as 802.11g or 802.11n.

For the best results, put your wireless router, wireless modem router (a DSL or cable modem with a built-in wireless router), or wireless access point (WAP) in a central location in your office. If your router is on the first floor and your devices are on the second floor, put the router high on a shelf on the first floor.

> ⓘ **Note**
>
> Metal objects, walls, and floors can interfere with your router's wireless signals.

Set up your modem and Internet connection

If your ISP didn't set up your modem, follow the instructions that came with your modem to connect it to your device and the Internet. If you're using a Digital Subscriber Line (DSL), connect your modem to a telephone jack. If you're using cable, connect your modem to a cable jack.

Set up a modem and router

To set up two pieces of hardware, a modem and a router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the modem and the other end into the wall jack. (DSL users shouldn't use a DSL filter on the phone line.)
3. Plug one end of an Ethernet cable into the modem and the other end into the wide area network (WAN) port on the router.
4. Plug the router into an electrical outlet.
5. Start (or restart) the device.
6. Now follow the instructions in the section below to complete the modem and router setup.

   > ⓘ **Note**
   >
   > Protect your router by changing the default user name and password. Most router manufacturers have a default user name and password on the router in addition to a default network name. Someone could use this information to access your router without your knowledge. Check the information that was included with your device for instructions.

Set up a combined modem and router

If you have a combined modem and router, follow these instructions:

1. Plug the modem into an electrical outlet.
2. Plug one end of a phone cord or cable into the wide area network (WAN) port of the device and the other into the wall jack. The WAN port should be labeled **WAN**. (DSL users shouldn't use a DSL filter on the phone line.)
3. Once completed, restart your device.

Complete the modem and router setup

To complete the modem and router setup， follow the instructions:

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network and Internet Connections**
4. Click **Set up or change your Internet connection** ****.
5. Click **Set up**.
6. Follow the instructions in the **New Connection Wizard** to connect to the Internet.
7. Follow the instructions in the wizard.

Set up your wireless network adapters

A network adapter connects your device to a network. To connect to a wireless network, your device must have a wireless network adapter. Make sure that you get the same type of adapters as your wireless router. The type of adapter is marked on the package with a letter, such as G or A.

To check whether your device has a wireless network adapter, follow the instructions.

1. Click **Start**, right-click **My Computer**, and then click **Properties**.
2. Under the **Hardware** tab, click **Device Manager**.
3. Next to **Network adapters**, click the plus sign (+).
4. Look for a network adapter that includes "wireless" in the name.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Set up a security key for your network

Every wireless network has a network security key to help protect it from unauthorized access.

To set up a network security key, follow the instructions.

1. Click **Next**.
2. Click **Start**.
3. Click **All Programs**.
4. Click **Accessories**.
5. Click **Communications**.
6. Click **Wireless Network Setup Wizard**.
7. In the open window, click **Next**.
8. Check on **Set up a new wireless network** and click **Next**.
9. Input the **Network name (SSID)**, check on **Manually assign a network key**, and click **Next**.
10. Input **Network key** and **Confirm network key** and click **Next**.
11. Check on **Set up a network manually** and click **Next**.
12. Click **Finish**.

Make sure that you write the security key and keep it in a safe place. If you have a USB flash drive, you can also save your security key to the flash drive by following the instructions in the wizard.

Set up a firewall

A firewall is hardware or software that helps control the spread of malicious software on your network and helps to protect your devices when you use the Internet. Don't turn off Windows Firewall unless you have another firewall turned on. Turning off Windows Firewall might make your device and network vulnerable to damage from hackers. To set up a firewall, follow the instructions:

1. Click **Start**.
2. Click **Run**.
3. Type **Firewall.cpl**, and click **OK**.
4. On the General tab, click **On** (recommended).
5. Click **OK**.

Enable file and printer sharing with a firewall

Windows Firewall automatically opens the correct ports for file and printer sharing when you share content or turn on network discovery. If you're using another firewall, you must open these ports yourself so that your device can find other devices that have files or printers that you want to share.

To find other devices running Windows 8, Windows 7, or Windows Vista, open these ports:

- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

To find other devices running earlier versions of Windows, and to use file and printer sharing on any version of Windows, open these ports:

- UDP 137
- UDP 138
- TCP 139
- TCP 445
- UDP 5355

To find network devices, open these ports:

- UDP 1900
- TCP 2869
- UDP 3702
- UDP 5355
- TCP 5357
- TCP 5358

Save your wireless network settings to a USB flash drive

1. Right-click the **Network** icon and click **Open Network and sharing Center**.
2. Click **Manage wireless networks**.
3. Right-click the network and click **Properties**.
4. Click **Copy this network profile to a USB flash drive**.
5. Select the USB device and click **Next**.
6. Follow the instructions in the wizard and then click **Close**.

Use a USB flash drive to connect to the network

If you want to use a USB flash drive to copy network settings to your device instead of typing a security key or passphrase, follow these steps:

1. Log on to the device that you want to add to the network.
2. Plug the USB flash drive that contains the network settings into a USB port on the device. For a device running Windows XP, in the **USB flash drive** dialog box, click **Wireless Network Setup Wizard**.

Connect devices to the network

To connect a device to your network, follow the instructions.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network Connections**.
4. Right-click **Wireless Network Connection**, and click **View Available Wireless Networks**.
5. Select the wireless network you want to connect to, and then click **Connect**.
6. Follow the steps in the wizard to configure the network.

For details on troubleshooting network connections for Windows XP devices, see Fix Wi-Fi connection issues in Windows.

Create and manage workgroups

A workgroup is a group of devices that are connected to a home or small office network and share resources, such as printers and files. When you set up a network, Windows automatically creates a workgroup and gives it a name. In a workgroup:

- All devices are peers; no device has control over another device.
- Each device has a set of user accounts. To log on to any device in the workgroup, you must have an account set up on it.
- There are typically no more than 20 devices in a workgroup.
- A workgroup isn't protected by a password.
- All devices must be on the same local network or subnet. If your network includes devices running different versions of Windows, you should put all the devices in the same workgroup so that they can find one another and easily share files and printers.

Find the default workgroup

To find a workgroup name, follow the instructions.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Type system in the Search box.
4. Tap or click **Settings**.
5. Tap or click **System** on the left side of your screen.
6. The workgroup name appears under **Device name, domain, and workgroup settings.**

Join or create a workgroup

To join or create a workgroup, follow the instructions.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Type system in the *Search* box.
4. Tap or click **Settings**.
5. Tap or click **System** on the left side of your screen.
6. Under **Device name, domain, and workgroup settings**, tap or click **Change settings**.

   > ⓘ **Note**
   >
   > You might be asked for an administrator password or to confirm your choice.

7. In **System Properties**, tap or click the **Device Name** tab and then tap or click **Change**.
8. In the **Device Name/Domain Changes** dialog box, tap or click **Workgroup** and then take one of the following actions:
   To join an existing workgroup, enter the name of the workgroup and tap or click **OK**.
   To create a new workgroup, enter a name for the workgroup and tap or click **OK**.
9. If your device was a member of a domain before you joined the workgroup, it will be removed from the domain and your device account on that domain will be disabled.

Change a workgroup name

If you want to change a workgroup name, follow these instructions:

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Type *System* in the Search box.
4. Tap or click **Settings**.
5. Tap or click **System** on the left side of your screen.
6. Under **Device name, domain, and workgroup settings**, tap or click **Change settings**.

   > ⓘ **Note**
   >
   > You might be asked for an administrator password or to confirm your choice.

7. In **System Properties**, tap or click the **Device Name** tab and then tap or click **Change**.
8. In the **Device Name/Domain Changes** dialog box, tap or click **Workgroup** and type the name of the workgroup you want to use.
9. Click **OK**.
10. Restart your device.

Find the default workgroup

To find a workgroup name, follow the instructions.

1. Click **Start**.
2. Right-click **My Device** and then click **Properties**.
3. The workgroup name appears under **Device name, domain, and workgroup settings**.

Join or create a workgroup

To join or create a workgroup, follow the instructions.

1. Click **Start**.
2. Right-click **My Device** and then click **Properties**.
3. Under **Device name, domain, and workgroup settings**, tap or click **Change settings**.

   > ⓘ **Note**

You might be asked for an administrator password or to confirm your choice.*

4. In **System Properties**, tap or click the **Device Name** tab and then tap or click **Change**.
5. In the **Device Name/Domain Changes** dialog box, under **Member of,** click **Workgroup** and select one of the following:
   To join an existing workgroup, enter the name of the workgroup and tap or click **OK**.
   To create a new workgroup, enter a name for the workgroup and tap or click **OK**.

Change a workgroup name

If you want to change a workgroup name, follow these instructions:

1. Click **Start**.
2. Right-click **My Device** and then click **Properties**.
3. Under **Device name, domain, and workgroup settings**, tap or click **Change settings**.
4. In **System Properties**, tap or click the Device Name tab and then tap or click **Change**.
5. In the **Device Name/Domain Changes in Workgroup**, type the name of the workgroup you want to use.
6. Click **OK**.
7. Restart your device.

Find the default workgroup

To find a workgroup name, follow the instructions.

1. Click **Start**.
2. Right-click **My Device** and then click **Properties**.
3. In **System Properties**, click the **Device Name** tab to see the workgroup name.
4. To change the workgroup name, click **Change**, type the new name in **Device name**, and click **OK**.

Join or create a workgroup

To join or create a workgroup, follow the instructions.

1. Click **Start**.
2. Right-click **My Device** and then click **Properties**.
3. From **System Properties**, click **Change**.

4. From the **Device Name Changes** dialog box, within the **Device Name** text box, type a device name. Within the **Workgroup** text box, enter the name of the workgroup.

   > ⓘ **Note**
   >
   > The Device Name for each device on the network must be unique, and the workgroup for all devices on the network must be the same.

5. Click **OK**.
6. From the **Device Name Changes** dialog box, click **OK**.
7. Restart your device.

Change a workgroup name

If you want to change a workgroup name, follow these instructions:

1. Click **Start**.
2. Right-click **My Device** and then click **Properties**.
3. From **System Properties**, click **Change**.
4. From the **Device Name Changes** dialog box, within the **Device Name** text box, type a device name. Within the **Workgroup** text box, enter the name of the workgroup.

   > ⓘ **Note**
   >
   > The Device Name for each device on the network must be unique, and the workgroup for all devices on the network must be the same.

5. Click **OK**.
6. From the **Device Name Changes** dialog box, click **OK**.
7. Restart your device.

Install a hybrid network

A hybrid network refers to any computer network that contains two or more communications standards such Ethernet (802.3) and Wi-Fi (802.11 a/b/g). A hybrid network relies on special hybrid routers, hubs, and switches to connect both wired and wireless computers and other network-enabled devices. It enables the network to maximize the benefits of both these network types.

Central access point

In a wired computer network, all devices are connected by physical cables to a central access point. This access point can be a router, hub, or a switch. The function of this access point is to share a network connection among several devices. All the devices are plugged into the access point using individual Ethernet (CAT 5) cables. If the devices need to share an Internet connection as well, then the access point is plugged into a broadband Internet modem, either cable or DSL.

In a standard wireless network, all networked devices communicate with a central wireless access point that broadcasts a signal. The devices themselves need to contain wireless modems or cards that conform with one or more Wi-Fi standards, either 802.11 a, b or g, to receive the signal. In this network configuration, all wireless devices can share files with each other over the network. If they also want to share an Internet connection, then the wireless access point is plugged into a broadband Internet modem.

A standard hybrid network uses a hybrid access point, a networking device that broadcasts a wireless signal and contains wired access ports. The most common hybrid access point is a hybrid router. The typical hybrid router broadcasts a Wi-Fi signal using 802.11 a, b, or g and contains four Ethernet ports for connecting wired devices. The hybrid router also has a port for connecting to a cable or DSL modem via an Ethernet cable.

When shopping for a hybrid router, you might not see the word "hybrid" anywhere. You're more likely to see the router advertised as a wireless or Wi-Fi router with Ethernet ports or "LAN ports".

After you determine which of your devices you want to connect with wires and which ones wirelessly, follow the procedures that are listed in **Install a wired network**, and **Install a wireless network** respectively to set up these parts of the hybrid network.

Network configurations

There are several different possible network configurations for a hybrid network. The most basic configuration has all the wired devices plugged into the Ethernet ports of the hybrid router, and the wireless devices connected to the router wirelessly. Then the wireless devices can communicate with the wired devices via the hybrid router.

If you want to network more than four wired devices, you can string several routers together, both wired and wireless, in a daisy chain formation. You'll need enough wired routers to handle all of the wired devices (the number of devices divided by four). And you'll need enough wireless routers in the right physical locations to broadcast a Wi-Fi

signal to every corner of the network. In this way, you can connect both computers and peripherals such as printers and fax machines and place them where it will easy to access them.

A hybrid wired/Wi-Fi network offers the best of both worlds: the speed and security of a wired network and the mobility and affordability of a wireless network. When you need the maximum Internet and file-sharing speed for your work, you can plug into the network with an Ethernet cable. If you need to show a streaming video to your colleague in the office hallway, you can access the network wirelessly. With the right planning, your small business can save money on CAT 5 cables and routers by maximizing the reach of the wireless network. And with the right encryption and password management in place, the wireless portion of the network can be as secure as the wired.

Share files and folders on your network

After you set up your network, you might want to add more sharing options for your work and devices. Some of these options are set automatically, while others can be set manually.

Sharing options for your device include:

- Finding other devices on your home network and having other devices find yours
- Sharing files and folders
- Sharing public folders

Sharing options that turn on automatically

In Windows 8.1 and Windows 8, when you connect to a network for the first time, you're given the option to turn on sharing and set the network location based upon your selection.

Sharing options that need to be turned on manually

If certain sharing options don't turn on automatically, you can activate them manually. These manual activation options include:

- Network discovery
- Network sharing (formerly location)
- Printer sharing
- File sharing

Network discovery

Network discovery is a network setting that lets your device find other devices on the network and other devices find your device. Such functionality makes it easier to share files and printers.

There are three network discovery states:

- **On:** Enables your device to see other network devices and people on other network devices to see your device.
- **Off:** Prevents your device from seeing other network devices and prevents people on other network devices from seeing your device.
- **Custom:** Enables limited network discovery. For example, if you run network discovery without meeting all required firewall conditions, the network discovery state would be shown as Custom.

To manually activate network discovery, follow the instructions.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Type *network and sharing center* in the Search box.
4. Tap or click **Settings**.
5. Tap or click **Network and Sharing Center** on the left side of your screen.
6. Tap or click **Change Advanced sharing settings** on the left pane.
7. Tap or click the chevron button to expand your current network profile.
8. Tap or click **Turn on network discovery** and then tap or click **Save changes**.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Network sharing (formerly network location)

Network sharing automatically adjusts security and other settings based on the type of network connected to your device. To check whether network sharing is enabled, follow the instructions.

The first time you connect to a network, you'll be asked if you want to turn on sharing between devices and connect to network devices such as printers. Your answer automatically sets the appropriate firewall and security settings for the type of network. You can turn sharing on or off at any time.

Turn sharing on or off in Windows 8.1 and Windows 8

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Settings**.
3. Tap or click the **Network** icon.
4. Press and hold or right-click the network name.
5. Tap or click **Turn sharing on or off**.
6. Select one of the following options:
   Yes, turn on sharing and connect to devices. Use this option for home or small office networks or when you know and trust the people and devices on the network.
   No, don't turn on sharing or connect to devices. Use this option for networks in public places (such as coffee shops or airports), or when you don't know or trust the people and devices on the network.

> ⓘ **Note**
>
> - Network sharing is only available for Wi-Fi, Ethernet, VPN (non-domain), and dial-up (non-domain) connections. It's unavailable for domain networks. On VPN or dial-up connections, you must connect to the network first, then press and hold or right-click the network name.
> - Turning on sharing changes your firewall settings to enable some communication, which can be a security risk. If you know you won't need to share files or printers, the safest choice is **No, don't sharing or connect to devices**.
> - Choosing **No, don't turn on sharing or connect to devices** blocks the following apps and services from working:
>
>   1. PlayTo
>   2. File sharing
>   3. Network discovery
>   4. Automatic setup of network devices

Printer Sharing

To manually activate printer sharing, follow the instructions.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Type **control panel** in the Search box.
4. Tap or click **Apps**.
5. Tap or click **Control Panel** on the left side of your screen.
6. Type Network and Sharing Center in the Search Control Panel box.
7. Tap or click **Network and Sharing Center**.
8. Tap or click **Change advanced sharing settings** on the left pane.
9. Check on **Turn on file and printer sharing**.
10. Tap or click **Save changes**.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Share a file or folder

To share a file or folder, follow the instructions for the version of Windows installed on your device.

1. Press and hold or right-click a file or folder.
2. Tap or click **Share with**.
3. Select the people or groups that you want to share with. You can also assign permissions so that those people can or can't change the file or folder shared.

Password-protected sharing

With password-protected sharing, people on your network can't access shared folders on other devices, including Public folders, unless they have a user name and password on the device for shared folders.

To activate password-protected sharing, follow the instructions.

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or click **Search**.
3. Type **control panel** in the Search box.
4. Tap or click **Apps**.
5. Tap or click **Control Panel** on the left side of your screen.
6. Type *Network and Sharing Center* in the search Control panel box.

7. Tap or click **Network and Sharing Center**.
8. Tap or click **Change advanced sharing settings** on the left pane.
9. Tap or click the arrow to expand your **All Network** profile.
10. Under **Password protected sharing**, tap or click **Turn on password protected sharing**.
11. Tap or click **Save changes**.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Network map

The network map is a graphical view of the devices and devices on your network. The map shows how devices are connected and includes any problem areas. It can be helpful for troubleshooting.

Windows 8.1 and Windows 8 don't have the network map feature.

Sharing options that turn on automatically

For Windows 7, certain sharing options turn on automatically. For example, when you change your network location to Home or Work, network discovery is automatically turned on. Similarly, file sharing turns on automatically the first time you try to share a file or folder.

Sharing options that need to be turned on manually

If certain sharing options don't turn on automatically, you can activate them manually. These manual activation options include:

- Network discovery
- Network sharing (formerly location)
- Printer sharing
- File sharing

Network discovery

Network discovery is a network setting that lets your device find other devices on the network and other devices find your device. Such functionality makes it easier to share

files and printers. There are three network discovery states:

- **On:** Enables your device to see other network devices and people on other network devices to see your device.
- **Off:** Prevents your device from seeing other network devices and prevents people on other network devices from seeing your device.
- **Custom:** Enables limited network discovery. For example, if you run network discovery without meeting all required firewall conditions, the network discovery state would be shown as Custom.

To manually activate network discovery, follow the instructions.

1. Click **Start**.
2. Click **Control Panel**.
3. Type network in the Search box.
4. Click **Network and Sharing Center** and then in the left pane, click **Change advanced sharing settings**.
5. Click the chevron button.
   to expand your current network profile.
6. Click **Turn on network discovery**.
7. Click **Save changes**.

Network sharing (formerly network location)

Windows 7 automatically adjusts security and other settings based on the type of network connected to your device. If you skip this step, then the first time that you connect to the network, you'll be asked to select your network location. You can change this setting later.

Check the network location devices

There are four network locations you can use for Windows 7 devices:

- **Home.** The network offers some protection from the Internet (such as a router and firewall) and contains known or trusted devices. Network discovery is turned on automatically.

- **Work.** The network offers some protection from the Internet (such as a router and firewall) and contains known or trusted devices. Network discovery is turned on automatically. Most small business networks fall into this category.

- **Public.** The network is available for public use. Examples of public networks are public Internet access networks, such as those found in airports, libraries, and

coffee shops. This network location helps keep your device from being seen by other devices around you and helps protect your device from malicious software on the Internet. You should also select this option if you're connected directly to the Internet without using a router or if you have a mobile broadband connection.

> ⓘ **Note**
>
> This is the safest setting, but you can't share printers or files.

- **Domain.** The device is connected to a network that contains an Active Directory domain controller. A corporate network is one example of a domain network. This network location isn't available as an option. It must be set by the domain administrator.

For your small business network, make sure that the network location type is set to Home or Work. Here's how to check:

1. Click **Start**.
2. Click **Control Panel**.
3. Type *network* in the Search box.
4. Click **Network and Sharing Center**.
5. In the left pane, click **Work network, Home network**, or **Public network**.
6. Click the network location that you want.

Printer Sharing

To manually activate printer sharing, follow the instructions.

1. Click **Start**.
2. Click **Devices and Printers** and then double-click your printer.
3. Click **Customize** your printer.
4. Click the **Sharing** tab and select the **Share this printer** check box.

Password-protected sharing

With password-protected sharing, people on your network can't access shared folders on other devices, including Public folders, unless they have a user name and password on the device for shared folders.

To activate password-protected sharing, follow the instructions.

1. Click **Start**.

2. Click **Control Panel**.
3. Type network in the Search box.
4. Click **Network and Sharing Center**.
5. In the left pane, click **Change advanced sharing settings**.
6. Click the arrow to expand the Home or Work network profile.
7. Under **Password protected sharing**, click **Turn on password protected sharing**.
8. Click **Save changes**.

> ⓘ **Note**
>
> You might be asked for an administrator password to confirm your choice.

Network map

The network map is a graphical view of the devices and devices on your network. The map shows how devices are connected and includes any problem areas. It can be helpful for troubleshooting.

The network map is available in the Network and Sharing Center on Windows 7.

Sharing options that turn on automatically

For Windows Vista, certain sharing options turn on automatically. For example, when you change your network location to Home or Work, network discovery is automatically turned on. Similarly, file sharing turns on automatically the first time you try to share a file or folder.

Sharing options that need to be turned on manually

If certain sharing options don't turn on automatically, you can activate them manually. These manual activation options include:

- Network discovery
- Network sharing (formerly location)
- Printer sharing
- File sharing

Network discovery

Network discovery is a network setting that lets your device find other devices on the network and other devices find your device. Such functionality makes it easier to share files and printers. There are three network discovery states:

- **On**: Enables your device to see other network devices and people on other network devices to see your device.
- **Off**: Prevents your device from seeing other network devices and prevents people on other network devices from seeing your device.
- **Custom**: Enables limited network discovery. For example, if you run network discovery without meeting all required firewall conditions, the network discovery state would be shown as Custom.

To manually activate network discovery, follow the instructions.

1. Click **Start**.
2. Click **Control Panel**.
3. Type network in the Search box.
4. Click **Network and Sharing Center** and then in the left pane, click **Change advanced sharing settings**.
5. Click the chevron button to expand your current network profile.
6. Click **Turn on network discovery**.
7. Click **Save changes**.

Network sharing (formerly network location)

Windows 7 automatically adjusts security and other settings based on the type of network connected to your device. If you skip this step, then the first time that you connect to the network, you'll be asked to select your network location. You can change this setting later.

Check the network location devices

- **Private**. For home or small office networks when you know and trust the people and devices on the network. Network discovery is on by default.

- **Public**. For networks in public places (such as coffee shops or airports). This location keeps your device from being visible to other devices around you and helps protect your device from any malicious software on the Internet. Network discovery is turned off for this location.

For your small business network, make sure that the network location type is set to Home or Work. Here's how to check:

1. Click **Start**.
2. Click **Control Panel**.
3. Type network in the Search box.
4. Click **Network and Sharing Center**.
5. Click **Customize** and then click **Public or Private**.
6. Click **Next**.
7. Click **Close**.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Printer Sharing

To manually activate printer sharing, follow the instructions.

1. Click **Start**.
2. Open the **Printers** control panel and right-click your printer.
3. Click **Sharing**.
4. Click **Change sharing** options.
5. Click **Continue**.
6. Click **Share this printer** and then click **OK**.

Share a file or folder

To share a file or folder, follow the instructions:

1. Press and hold or right-click a file or folder.
2. Tap or click **Share with**.
3. Select the people or groups that you want to share with. You can also assign permissions so that those people can or can't change the file or folder shared.

Password-protected sharing

With password-protected sharing, people on your network can't access shared folders on other devices, including Public folders, unless they have a user name and password on the device for shared folders.

To activate password-protected sharing, follow the instructions.

1. Click **Start**.

2. Click **Control Panel**.
3. Type network in the Search box.
4. Open **Network and Sharing Center** in **Control Panel**.
5. Under **Sharing and Discovery**, click the chevron next to **Password protected sharing** to expand the section.
6. Click **Turn on password protected sharing**.
7. Click **Apply**.

> ⓘ **Note**
>
> You might be asked for an administrator password or to confirm your choice.

Network map

The network map is a graphical view of the devices and devices on your network. The map shows how devices are connected and includes any problem areas. It can be helpful for troubleshooting.

The network map is available in the Network and Sharing Center on Windows Vista.

Sharing options that turn on automatically

In Windows XP, password-protected file sharing is turned on by default.

> ⓘ **Note**
>
> Windows XP only detects and accesses devices that are in the same workgroup.

Sharing options that need to be turned on manually

If certain sharing options don't turn on automatically, you can activate them manually. These manual activation options include:

- Network discovery
- Network sharing (formerly location)
- Printer sharing
- File sharing

Network discovery

Network discovery is a network setting that lets your device find other devices on the network and other devices find your device. Such functionality makes it easier to share files and printers. There are three network discovery states:

- **On**: Enables your device to see other network devices and people on other network devices to see your device.
- **Off**: Prevents your device from seeing other network devices and prevents people on other network devices from seeing your device.
- **Custom**: Enables limited network discovery. For example, if you run network discovery without meeting all required firewall conditions, the network discovery state would be shown as Custom.

To ensure that a Windows XP device displays on the network, install the Link-Layer Topology Discovery (LLTD) protocol on the device. If this operation doesn't resolve the problem, enable file and printer sharing, and NETBIOS.

1. Click **Start**.
2. Click **Control Panel**.
3. Click **Network Connections**.
4. Select the network connection for your network.
5. If the device you're on doesn't display, select the checkbox for **File and Printer Sharing for Microsoft Networks**.
6. Click **Close**.

> ⓘ **Note**
>
> Windows XP only detects and accesses devices that are in the same workgroup.

Printer Sharing

To manually activate printer sharing, follow the instructions.

1. Open the **Printers and Faxes** control panel and right-click your printer.
2. Click **Share this printer** and then click **OK**.

> ⓘ **Note**
>
> If your network consists of devices that are running similar hardware and software, you can select the option to download additional printer drivers on the host

system. We do not recommend this option if you have a mixed network that includes more than one combination of 32-bit and 64-bit operating systems.

Share a file or folder

To share a file or folder, follow the instructions.

1. Click **Sharing and Security**.
2. Select the people or groups that you want to share with. You can also assign permissions so that those people can or can't change to the file or folder you shared.

> **Note**
>
> If your network contains devices running different versions of Windows, put all devices in the same workgroup. This makes it possible for devices that are running different versions of Windows to detect and access one another. Remember that the default workgroup name is not the same in all versions of Windows.

Password-protected sharing

With password-protected sharing, people on your network can't access shared folders on other devices, including Public folders, unless they have a user name and password on the device for shared folders.

With Windows XP, password protected sharing is turned on by default.

Network map

The network map is a graphical view of the devices and devices on your network. The map shows how devices are connected and includes any problem areas. It can be helpful for troubleshooting.

If you want a device running Windows XP to appear on the network map, you might have to install the Link-Layer Topology Discovery (LLTD) protocol on that device.

If Windows XP devices still don't appear on the network map even after you install the LLTD protocol, check your Windows firewall settings and make sure that file and printer sharing is enabled. "To learn more about this issue, open **Help and Support** and search

for *Enable file and printer sharing*". If you're using another firewall, see the information that was included with your firewall.

Settings for minimizing periodic WAN traffic

Article • 08/31/2022 • 10 minutes to read

This article provides some suggested settings for the problem that occurs when a dial-on-demand link is activated by periodic WAN traffic.

Applies to: Windows Server 2016, Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 819108

Summary

This article describes the registry settings and the Group Policy settings that affect periodic wide area network (WAN) traffic and metered link costs. If you have a dial-on-demand link, it might be unexpectedly enabled by periodic WAN traffic. You can configure the system's components and services to minimize periodic WAN traffic and to reduce metered link costs.

Symptoms

Your dial-on-demand link activates while the computer is idle if the following conditions are true:

- You are using a Microsoft Windows-based computer that's connected to a remote network and is a member of an Active Directory Domain Services (AD DS) domain.
- You are connected to the domain controllers over a dial-on-demand or otherwise metered link.

Resolution

The following sections contain a comprehensive summary of registry settings and Group Policy settings that you can add or modify to minimize WAN traffic. Some of these settings depend on the operating system version that the computer is running.

Part 1: A description of relevant settings

The following registry settings affect WAN traffic and metered-link costs. To minimize periodic WAN traffic and to reduce metered link costs, configure these settings as appropriate.

The Browser service

In Windows Server 2016, Windows 10, and later versions, the Browser service is generally no longer used. We recommend that you disable the service on all computers in your enterprise, if it is possible. If you can't do this, we recommend you turn down the communication intervals of the service.

The domain master browser periodicity

The primary domain controller (PDC) is always the domain master browser. Therefore, a master browser on a network that does not host the PDC for the domain activates dial-on-demand links when it tries to locate the PDC. By default, the attempt interval is five minutes. You can create a **MasterPeriodicity** registry entry that instructs the Browser service to adjust its default interval for contacting a domain master browser. By default, the **MasterPeriodicity** entry is not present. The recommended default for dial-on-demand deployments is **86,400** seconds (one day).

Subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\Parameters`
Entry: MasterPeriodicity

Type: DWORD
Recommended value (seconds): 86,400

Server list maintenance

If you enable a server to participate as a browser and to potentially be elected as a master browser for its network, the server periodically contacts the PDC for its domain. By default, the **MaintainServerList** registry entry is set to **Auto**. The recommended value is **No** unless you must have browser functionality on the network. If you must have browser functionality, set this value to **Yes**. However, make sure to configure the **MasterPeriodicity** interval to a large enough interval to reduce the number of PDC contacts.

Subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\Parameters`
Entry: MaintainServerList
Type: String Default value: Auto
Recommended value: No

The expected dial-up delay

The **ExpectedDialupDelay** entry specifies the time that is required for a dial-up router to dial when it sends a message from a client computer to a domain across a slow link. In this scenario, the domain is trusted by the client computer. Typically, the Net Logon service assumes that it can quickly reach a domain controller. By setting the **ExpectedDialupDelay** entry, you inform the Net Logon service to expect an additional delay. The recommended value for this setting is the average time in seconds that is required for the dial-on-demand link to be established, plus a constant of five seconds to account for variance.

Subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
Entry: ExpectedDialupDelay
Type: DWORD
Recommended value (seconds): 90

The AvoidPdcOnWan entry

The **AvoidPdcOnWan** entry instructs the domain controller that is running the Net Logon service to avoid contacting the PDC operations master roles as much as it can. (The operations master roles are also known as flexible single master operations roles or FSMO roles.) The **AvoidPdcOnWan** entry also instructs other components, such as the Security Account Manager (SAM), that use this information. For example, assume that this entry is enabled on a domain controller in a remote site. In this scenario, the remote domain controller will not try to verify a password with the PDC operations master roles if the client does not authenticate with the local domain controller.

Subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
Entry: AvoidPdcOnWan
Type: DWORD
Recommended value: 1 (enabled)

Directory service client queries

In Windows 2000 Service Pack 2 and in later Windows 2000 service packs, in Windows XP, and in Windows Server 2003, the Directory service client queries are issued one time per hour. You can adjust the following registry entries to extend this query time beyond one hour.

The negative cache period

The **NegativeCachePeriod** entry specifies the time that a client will remember that a domain controller could not be found in a domain. If a program tries again within this time, the client call immediately fails without trying to find a domain controller again, so the metered link is not activated.

Subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
Entry: NegativeCachePeriod
Type: DWORD
Default value (seconds): 45
Recommended value: 84,600

The background retry initial period

Some programs periodically try to find a domain controller. If the domain controller is not available, these periodic retries can be costly in dial-on-demand scenarios. The **BackgroundRetryInitialPeriod** entry defines the minimum amount of elapsed time before the first retry occurs. If the value is smaller than the value set in the **NegativeCachePeriod** entry, the **NegativeCachePeriod** value is used.

Subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
Entry: BackgroundRetryInitialPeriod
Type: DWORD
Recommended value (seconds): 84,600

The background retry back-off period

The **BackgroundRetryMaximumPeriod** entry defines the maximum interval that the retries will be backed off. For example, if the first retry is after 10 minutes, the second retry will be after 20 minutes, and the next retry will be after 30 minutes. This continues until the value in the **BackgroundRetryMaximumPeriod** entry is reached. Then, the **BackgroundRetryBackoffPeriod** value is used for the retry interval until the value in the **BackgroundRetryQuitTime** entry is reached.

Subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
Entry: BackgroundRetryMaximumPeriod
Type: DWORD
Recommended value (seconds): 84,600 seconds

The background retry quit time

When a program runs a periodic search for domain controllers and cannot find a domain controller, the value that is set in this entry determines when retries are no longer possible.
Subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
Entry: BackgroundRetryQuitTime
Type: DWORD
Recommended value (seconds): 600

The maximum password age

Specifies how frequently the system changes the computer account password of the local computer. This entry is used only when the system is configured to change the computer password automatically at set intervals. That is, this entry is used only when the value of the **DisablePasswordChange** entry is **0**. For more information, see Domain member: Disable machine account password changes.

Subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
Entry: MaximumPasswordAge
Type: DWORD

Default value (decimal, number of days): 7 (in Windows NT), 30 (Windows 2000/XP/2003) Recommended range: 42 to 70

DFS registry settings

The frequency of domain controller queries by DFS the **DfsDcNameDelay** entry can reduce the frequency of domain controller queries by Distributed File System (DFS). Modify this entry on the client computer.

Subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters`
Entry: DfsDcNameDelay
Type: DWORD
Default value (minutes): 15

The valid range for **DfsDcNameDelay** is from **15** to **360** minutes. No restart is required for the new settings to take effect.

The frequency of PDC queries by DFS

Description: Every DFS server that has a domain-based DFS root polls the PDC for changes on the root object. You can control the interval between pollings by setting the **SyncIntervalInSeconds** registry entry on the DFS root server or servers. By setting this entry, you can control when DFS returns referrals that are based on cached data. If you increase this value, DFS caches namespaces and referrals for a longer duration.

Subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DFS`
Entry: SyncIntervalInSeconds
Type: DWORD
Default value (seconds): 3,600 (1 hour)

Also review the following technical article on DFS volume settings:

- Change the amount of time that clients cache referrals

The Knowledge Consistency Checker (KCC) replication topology update

The Knowledge Consistency Checker (KCC) replication topology update may cause WAN traffic to create or verify replication links. For domain controllers that are separated by metered links, it makes sense to reduce the frequency at which KCC runs.

Description: The Repl topology update period (secs) value defines the number of seconds between intervals.

Subkey: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters`
Entry: Repl topology update period (secs)
Type: DWORD
Default value (seconds): 900 (15 minutes)

Group Policy settings

The following policy settings control the frequency of Net Logon-based traffic and of DFS-based traffic. To locate these settings, click **Start**, click **Run**, type *gpedit.msc*, and then click **OK**. Or, edit them in a domain-based Group Policy Object.

Computer Configuration/Administrative Templates/System/Net Logon

- **Scavenge Interval**
- **Positive Periodic DC Cache Refresh for Non-Background Callers**
- **Positive Periodic DC Cache Refresh for Background Callers**

- **Final DC Discovery Retry Settings for Background Callers**
- **Maximum DC Discovery Retry Interval Settings for Background Callers**
- **Initial DC Discovery Retry Settings for Background Callers**
- **Negative DC Discovery Cache Settings**
- **Contact PDC on logon failure**
- **Expected dial-up delay on logon**

Computer Configuration/Administrative Templates/Network

Sets how often a DFS Client discovers DCs

By default, a DFS client tries to discover domain controllers every 15 minutes. If you enable the **Sets how often a DFS Client discovers DCs** setting, you can change the interval. This value is specified in minutes. If you disable this setting or do not configure it, the default value of 15 minutes applies. The corresponding registry subkey is as follows: `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\System\DFSClient\DfsDcNameDelay`

Part 2: Default values

Default values for packet types

The following table shows the packet types and their default send intervals.

Packet type	Protocol	Transport	Interval	Notes
NetLogon	Server message block (SMB)	TCP/IP	300 seconds	
Browse	SMB	TCP/IP	720 seconds	
KeepAlive	Network basic input/output system (NetBIOS)	TCP/IP	3,600 seconds (60 minutes)	
Echo NetBIOS over TCP/IP (NetBT)	NetBIOS	TCP/IP	120 seconds	If a session is idle, the file server sends an SMB echo frame at the specified interval.
Windows Explorer	SMB	TCP/IP	32 seconds	This value controls the frequency that the file server sends an SMB echo frame to the client as long as the client has an outstanding long-term request open.
KeepAlive	NetBIOS	TCP/IP	300 seconds (5 minutes)	This entry corresponds to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlServices\NetBT\parameters\SessionKeepAlive`
KeepAlive	TCP	TCP/IP	1 second	This entry corresponds to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP\Parameters\KeepAliveTime`

> ⓘ Note
>
> - The Browse packet type in this table indicates network traffic between a PDC (Domain Master Browser) and master browsers.

- The Windows LAN Manager redirector echoes an SMB echo frame every 30 seconds or 32 seconds to each file server that has an associated long-term request that is outstanding. For example, a file server might have a **NotifyChange** request in Microsoft Internet Explorer. To avoid these packets, you can set the **NoRemoteChangeNotify** key.

For more information, see the following Knowledge Base article: 3212430 Security setting changes on folders don't appear immediately on DFSR replication partners in Windows Server

- If there is no data transfer between the client and the server for the KeepAlive interval (120 seconds), the server sends the first keep-alive probe. After two minutes of inactivity (idle tree connects), the file server sends a 1-byte session message. The TCP payload is "02." The TCP sequence number starts in the last received acknowledgment (ACK) minus 1 and ends in the current acknowledgment.
- If the connection against the server is made by using named pipes, the server sends a "NetBT: SS - Session Keep Alive" message to the client approximately every 300 seconds.

  The "NetBT SessionKeepAlive" entry is in the following registry subkey:
  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters`
- A Common Internet File System (CIFS) TCP session keep-alive message includes a byte that has a 0x85 value, followed by three bytes that have a 0 (zero) value in the NetBT header. The keep-alive message may be sent if no messages have been sent for a client-configurable interval.

Default values for services

Component	Default interval setting	Notes
The Net Logon domain controller discovery	3,600 seconds (60 minutes)	
DFS queries for domain controllers	900 seconds (15 minutes)	
GPO refresh interval	90 minutes	See Group Policy Description: Group Policy Search

Time service (W32time)	17 minutes	This value is found in the following registry subkeys:
		`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32time\Config\MaxPollInterval`
		`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32time\Config\MinPollInterval`
		Also see the Group Policy settings for Windows Time Service: Global Configuration Settings
		Configure Windows NTP Client

References

For more information, see the following Knowledge Base articles:

- 314053 TCP/IP and NBT configuration parameters for Windows XP
- 3212430 Security setting changes on folders don't appear immediately on DFSR replication partners in Windows Server

Understand TCP/IP addressing and subnetting basics

Article • 12/27/2022 • 12 minutes to read

This article is intended as a general introduction to the concepts of Internet Protocol (IP) networks and subnetting. A glossary is included at the end of article.

Applies to: Windows 10 - all editions
Original KB number: 164015

Summary

When you configure the TCP/IP protocol on a Windows computer, the TCP/IP configuration settings require:

- An IP address
- A subnet mask
- A default gateway

To configure TCP/IP correctly, it's necessary to understand how TCP/IP networks are addressed and divided into networks and subnetworks.

The success of TCP/IP as the network protocol of the Internet is largely because of its ability to connect together networks of different sizes and systems of different types. These networks are arbitrarily defined into three main classes (along with a few others) that have predefined sizes. Each of them can be divided into smaller subnetworks by system administrators. A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs. To better understand how IP addresses and subnet masks work, look at an IP address and see how it's organized.

IP addresses: Networks and hosts

An IP address is a 32-bit number. It uniquely identifies a host (computer or other device, such as a printer or router) on a TCP/IP network.

IP addresses are normally expressed in dotted-decimal format, with four numbers separated by periods, such as 192.168.123.132. To understand how subnet masks are used to distinguish between hosts, networks, and subnetworks, examine an IP address in binary notation.

For example, the dotted-decimal IP address 192.168.123.132 is (in binary notation) the 32-bit number 11000000101010000111101110000100. This number may be hard to make sense of, so divide it into four parts of eight binary digits.

These 8-bit sections are known as octets. The example IP address, then, becomes 11000000.10101000.01111011.10000100. This number only makes a little more sense, so for most uses, convert the binary address into dotted-decimal format (192.168.123.132). The decimal numbers separated by periods are the octets converted from binary to decimal notation.

For a TCP/IP wide area network (WAN) to work efficiently as a collection of networks, the routers that pass packets of data between networks don't know the exact location of a host for which a packet of information is destined. Routers only know what network the host is a member of and use information stored in their route table to determine how to get the packet to the destination host's network. After the packet is delivered to the destination's network, the packet is delivered to the appropriate host.

For this process to work, an IP address has two parts. The first part of an IP address is used as a network address, the last part as a host address. If you take the example 192.168.123.132 and divide it into these two parts, you get 192.168.123. Network .132 Host or 192.168.123.0 - network address. 0.0.0.132 - host address.

Subnet mask

The second item, which is required for TCP/IP to work, is the subnet mask. The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network.

In TCP/IP, the parts of the IP address that are used as the network and host addresses aren't fixed. Unless you have more information, the network and host addresses above can't be determined. This information is supplied in another 32-bit number called a subnet mask. The subnet mask is 255.255.255.0 in this example. It isn't obvious what this number means unless you know 255 in binary notation equals 11111111. So, the subnet mask is 11111111.11111111.11111111.00000000.

Lining up the IP address and the subnet mask together, the network, and host portions of the address can be separated:

11000000.10101000.01111011.10000100 - IP address (192.168.123.132)
11111111.11111111.11111111.00000000 - Subnet mask (255.255.255.0)

The first 24 bits (the number of ones in the subnet mask) are identified as the network address. The last 8 bits (the number of remaining zeros in the subnet mask) are

identified as the host address. It gives you the following addresses:

11000000.10101000.01111011.00000000 - Network address (192.168.123.0)
00000000.00000000.00000000.10000100 - Host address (000.000.000.132)

So now you know, for this example using a 255.255.255.0 subnet mask, that the network ID is 192.168.123.0, and the host address is 0.0.0.132. When a packet arrives on the 192.168.123.0 subnet (from the local subnet or a remote network), and it has a destination address of 192.168.123.132, your computer will receive it from the network and process it.

Almost all decimal subnet masks convert to binary numbers that are all ones on the left and all zeros on the right. Some other common subnet masks are:

Decimal	Binary
255.255.255.192	1111111.11111111.1111111.11000000
255.255.255.224	1111111.11111111.1111111.11100000

Internet RFC 1878 (available from InterNIC-Public Information Regarding Internet Domain Name Registration Services) describes the valid subnets and subnet masks that can be used on TCP/IP networks.

Network classes

Internet addresses are allocated by the InterNIC , the organization that administers the Internet. These IP addresses are divided into classes. The most common of them are classes A, B, and C. Classes D and E exist, but aren't used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of Class A, B, and C Internet addresses, each with an example address:

- Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.
- Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.
- Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

In some scenarios, the default subnet mask values don't fit the organization needs for one of the following reasons:

- The physical topology of the network
- The numbers of networks (or hosts) don't fit within the default subnet mask restrictions.

The next section explains how networks can be divided using subnet masks.

Subnetting

A Class A, B, or C TCP/IP network can be further divided, or subnetted, by a system administrator. It becomes necessary as you reconcile the logical address scheme of the Internet (the abstract world of IP addresses and subnets) with the physical networks in use by the real world.

A system administrator who is allocated a block of IP addresses may be administering networks that aren't organized in a way that easily fits these addresses. For example, you have a wide area network with 150 hosts on three networks (in different cities) that are connected by a TCP/IP router. Each of these three networks has 50 hosts. You are allocated the class C network 192.168.123.0. (For illustration, this address is actually from a range that isn't allocated on the Internet.) It means that you can use the addresses 192.168.123.1 to 192.168.123.254 for your 150 hosts.

Two addresses that can't be used in your example are 192.168.123.0 and 192.168.123.255 because binary addresses with a host portion of all ones and all zeros are invalid. The zero address is invalid because it's used to specify a network without specifying a host. The 255 address (in binary notation, a host address of all ones) is used to broadcast a message to every host on a network. Just remember that the first and last address in any network or subnet can't be assigned to any individual host.

You should now be able to give IP addresses to 254 hosts. It works fine if all 150 computers are on a single network. However, your 150 computers are on three separate physical networks. Instead of requesting more address blocks for each network, you divide your network into subnets that enable you to use one block of addresses on multiple physical networks.

In this case, you divide your network into four subnets by using a subnet mask that makes the network address larger and the possible range of host addresses smaller. In other words, you are 'borrowing' some of the bits used for the host address, and using them for the network portion of the address. The subnet mask 255.255.255.192 gives you four networks of 62 hosts each. It works because in binary notation, 255.255.255.192

is the same as 1111111.11111111.1111111.11000000. The first two digits of the last octet become network addresses, so you get the additional networks 00000000 (0), 01000000 (64), 10000000 (128) and 11000000 (192). (Some administrators will only use two of the subnetworks using 255.255.255.192 as a subnet mask. For more information on this topic, see RFC 1878.) In these four networks, the last six binary digits can be used for host addresses.

Using a subnet mask of 255.255.255.192, your 192.168.123.0 network then becomes the four networks 192.168.123.0, 192.168.123.64, 192.168.123.128 and 192.168.123.192. These four networks would have as valid host addresses:

192.168.123.1-62 192.168.123.65-126 192.168.123.129-190 192.168.123.193-254

Remember, again, that binary host addresses with all ones or all zeros are invalid, so you can't use addresses with the last octet of 0, 63, 64, 127, 128, 191, 192, or 255.

You can see how it works by looking at two host addresses, 192.168.123.71 and 192.168.123.133. If you used the default Class C subnet mask of 255.255.255.0, both addresses are on the 192.168.123.0 network. However, if you use the subnet mask of 255.255.255.192, they are on different networks; 192.168.123.71 is on the 192.168.123.64 network, 192.168.123.133 is on the 192.168.123.128 network.

Default gateways

If a TCP/IP computer needs to communicate with a host on another network, it will usually communicate through a device called a router. In TCP/IP terms, a router that is specified on a host, which links the host's subnet to other networks, is called a default gateway. This section explains how TCP/IP determines whether or not to send packets to its default gateway to reach another computer or device on the network.

When a host attempts to communicate with another device using TCP/IP, it performs a comparison process using the defined subnet mask and the destination IP address versus the subnet mask and its own IP address. The result of this comparison tells the computer whether the destination is a local host or a remote host.

If the result of this process determines the destination to be a local host, then the computer will send the packet on the local subnet. If the result of the comparison determines the destination to be a remote host, then the computer will forward the packet to the default gateway defined in its TCP/IP properties. It's then the responsibility of the router to forward the packet to the correct subnet.

Troubleshooting

TCP/IP network problems are often caused by incorrect configuration of the three main entries in a computer's TCP/IP properties. By understanding how errors in TCP/IP configuration affect network operations, you can solve many common TCP/IP problems.

Incorrect Subnet Mask: If a network uses a subnet mask other than the default mask for its address class, and a client is still configured with the default subnet mask for the address class, communication will fail to some nearby networks but not to distant ones. As an example, if you create four subnets (such as in the subnetting example) but use the incorrect subnet mask of 255.255.255.0 in your TCP/IP configuration, hosts won't be able to determine that some computers are on different subnets than their own. In this situation, packets destined for hosts on different physical networks that are part of the same Class C address won't be sent to a default gateway for delivery. A common symptom of this issue is when a computer can communicate with hosts that are on its local network and can talk to all remote networks except those networks that are nearby and have the same class A, B, or C address. To fix this problem, just enter the correct subnet mask in the TCP/IP configuration for that host.

Incorrect IP Address: If you put computers with IP addresses that should be on separate subnets on a local network with each other, they won't be able to communicate. They'll try to send packets to each other through a router that can't forward them correctly. A symptom of this problem is a computer that can talk to hosts on remote networks, but can't communicate with some or all computers on their local network. To correct this problem, make sure all computers on the same physical network have IP addresses on the same IP subnet. If you run out of IP addresses on a single network segment, there are solutions that go beyond the scope of this article.

Incorrect Default Gateway: A computer configured with an incorrect default gateway can communicate with hosts on its own network segment. But it will fail to communicate with hosts on some or all remote networks. A host can communicate with some remote networks but not others if the following conditions are true:

- A single physical network has more than one router.
- The wrong router is configured as a default gateway.

This problem is common if an organization has a router to an internal TCP/IP network and another router connected to the Internet.

References

Two popular references on TCP/IP are:

- "TCP/IP Illustrated, Volume 1: The Protocols," Richard Stevens, Addison Wesley, 1994
- "Internetworking with TCP/IP, Volume 1: Principles, Protocols, and Architecture," Douglas E. Comer, Prentice Hall, 1995

It is recommended that a system administrator responsible for TCP/IP networks have at least one of these references available.

Glossary

- Broadcast address--An IP address with a host portion that is all ones.
- Host--A computer or other device on a TCP/IP network.
- Internet--The global collection of networks that are connected together and share a common range of IP addresses.
- InterNIC--The organization responsible for administration of IP addresses on the Internet.
- IP--The network protocol used for sending network packets over a TCP/IP network or the Internet.
- IP Address--A unique 32-bit address for a host on a TCP/IP network or internetwork.
- Network--There are two uses of the term network in this article. One is a group of computers on a single physical network segment. The other is an IP network address range that is allocated by a system administrator.
- Network address--An IP address with a host portion that is all zeros.
- Octet--An 8-bit number, 4 of which comprise a 32-bit IP address. They have a range of 00000000-11111111 that correspond to the decimal values 0-255.
- Packet--A unit of data passed over a TCP/IP network or wide area network.
- RFC (Request for Comment)--A document used to define standards on the Internet.
- Router--A device that passes network traffic between different IP networks.
- Subnet Mask--A 32-bit number used to distinguish the network and host portions of an IP address.

- Subnet or Subnetwork--A smaller network created by dividing a larger network into equal parts.
- TCP/IP--Used broadly, the set of protocols, standards, and utilities commonly used on the Internet and large networks.
- Wide area network (WAN)--A large network that is a collection of smaller networks separated by routers. The Internet is an example of a large WAN.

TCP/IP and NBT configuration parameters for Windows XP

Article • 03/04/2022 • 28 minutes to read

This article defines all the registry parameters that are used to configure the protocol driver, Tcpip.sys. Tcpip.sys implements the standard TCP/IP network protocols.

Applies to: Windows XP
Original KB number: 314053

Introduction

The TCP/IP protocol suite implementation for Windows XP reads all its configuration data from the registry. This information is written to the registry by the Network tool in Control Panel as part of the Setup process. Some of this information is also supplied by the Dynamic Host Configuration Protocol (DHCP) Client service if the DHCP Client service is enabled.

The implementation of the protocol suite should perform correctly and efficiently in most environments by using only the configuration information that is gathered by DHCP and by the Network tool in Control Panel. Optimal default values for all other configurable aspects of the protocols have been encoded in the drivers.

There may be some unusual circumstances in customer installations where changes to certain default values are appropriate. To handle these cases, optional registry parameters can be created to modify the default behavior of some parts of the protocol drivers.

> **Note**
>
> The Windows XP TCP/IP implementation is largely self-tuning. Adjusting registry parameters without careful study may reduce your computer's performance.

How to change parameters

> **Important**

This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

To change these parameters, follow these steps:

1. Click **Start**, click **Run**, and then type *regedit* in the **Open** box.
2. Locate the following registry key:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`
3. Click **Add Value** on the **Edit** menu, type the value that you want, and then set the value type under **Data Type**.
4. Click **OK**.
5. Quit Registry Editor.
6. Restart the computer to make the change take effect.

All the TCP/IP parameters are registry values that are located under one of two different subkeys of `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`:

- `Tcpip\Parameters`
- `Tcpip\Parameters\Interfaces\ID for Adapter`

> ⓘ Note
>
> **ID for Adapter** is the network adapter that TCP/IP is bound to. To determine the relationship between an Adapter ID and a network connection, view `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}\<ID for Adapter>\Connection`. The Name value in these keys provides the friendly name for a network connection that is used in the Network Connections folder. Values under these keys are specific to each adapter. Parameters that have a DHCP configured value and a statically configured value may or may not exist. Their existence depends on whether the computer or the adapter is DHCP configured and whether static override values are specified. You must restart the computer for a change to take effect.

Standard TCP/IP parameters that you can configure by using Registry Editor

The following parameters are installed with default values by the Network tool in Control Panel during the installation of the TCP/IP components. You can use Registry Editor to modify them.

- DatabasePath
  - Key: `Tcpip\Parameters`
  - Value type: REG_EXPAND_SZ - Character string
  - Valid range: A valid Windows NT file path
  - Default: %SystemRoot%\System32\Drivers\Etc
  - Description: This parameter specifies the path of the standard Internet database files (HOSTS, LMHOSTS, NETWORKS, PROTOCOLS). It is used by the Windows Sockets interface.

- ForwardBroadcasts
  - Key: `Tcpip\Parameters`
  - Value type: REG_DWORD - Boolean
  - Valid range: 0 or 1 (False or True)
  - Default: 0 (False)
  - Description: Forwarding of broadcasts is not supported. This parameter is ignored.

- UseZeroBroadcast
  - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
  - Value type: REG_DWORD - Boolean
  - Valid range: 0 or 1 (False or True)
  - Default: 0 (False)
  - Description: If this parameter is set to 1 (True), the IP will use zeros-broadcasts (0.0.0.0) instead of ones-broadcasts (255.255.255.255). Most computers use ones-broadcasts, but some computers that are derived from BSD implementations use zeros-broadcasts. Computers that use different broadcasts do not interoperate well on the same network.

Optional TCP/IP parameters that you can configure by using Registry Editor

Generally, these parameters do not exist in the registry. You can create them to modify the default behavior of the TCP/IP protocol driver.

- ArpAlwaysSourceRoute
  - Key: `Tcpip\Parameters`
  - Value type: REG_DWORD - Boolean

    - Valid range: 0,1 (False or True)
    - Default: 0 (False)
    - Description: If you set this parameter to 1, TCP/IP transmits ARP queries with source routing enabled on Token Ring networks. By default, the stack transmits ARP queries without source routing first and retries with source routing enabled if no reply was received.

- ArpUseEtherSNAP
    - Key: `Tcpip\Parameters`
    - Value type: REG_DWORD - Boolean
    - Valid range: 0,1 (False or True)
    - Default: 0 (False)
    - Description: If you set this parameter to 1, TCP/IP transmits Ethernet packets using 802.3 SNAP encoding. By default, the stack transmits packets in DIX Ethernet format. It will always receive both formats.

- DefaultTTL
    - Key: `Tcpip\Parameters`
    - Value type: REG_DWORD - Number of seconds/hops
    - Valid range: 1-255
    - Default: 128 for Windows XP
    - Description: This parameter specifies the default Time To Live (TTL) value that is set in the header of outgoing IP packets. The TTL determines the maximum time that an IP packet can live in the network without reaching its destination. It is effectively a limit on the number of routers an IP packet can pass through before it is discarded.

- EnableDeadGWDetect
    - Key: `Tcpip\Parameters`
    - Value type: REG_DWORD - Boolean
    - Valid range: 0,1 (False, True)
    - Default: 1 (True)
    - Description: If you set this parameter to 1, TCP uses the Dead Gateway Detection feature. With this feature, TCP requests IP to change to a backup gateway if it retransmits a segment several times without receiving a response. Backup gateways may be defined in the **Advanced** section of the **TCP/IP configuration** dialog box in the Network Control Panel.

- EnablePMTUBHDetect
    - Key: `Tcpip\Parameters`
    - Value type: REG_DWORD - Boolean
    - Valid range: 0,1 (False, True)

    - Default: 0 (False)
    - Description: If you set this parameter to 1 (True), TCP tries to detect "Black Hole" routers while doing Path MTU Discovery. A "Black Hole" router does not return ICMP Destination Unreachable messages when it must fragment an IP datagram with the Don't Fragment bit set. TCP must receive these messages to perform Path MTU Discovery. With this feature enabled, TCP will try to send segments without the Don't Fragment bit set if several retransmissions of a segment are unacknowledged. If the segment is acknowledged, the MSS will be decreased and the Don't Fragment bit will be set in future packets on the connection. Enabling black hole detection increases the maximum number of retransmissions that are performed for a particular segment.

- EnablePMTUDiscovery
    - Key: `Tcpip\Parameters`
    - Value type: REG_DWORD - Boolean
    - Valid range: 0,1 (False, True)
    - Default: 1 (True)
    - Description: If you set this parameter to 1 (True), TCP tries to discover the Maximum Transmission Unit (MTU or largest packet size) over the path to a remote host. By discovering the Path MTU and limiting TCP segments to this size, TCP can eliminate fragmentation at routers along the path that connect networks with different MTUs. Fragmentation adversely affects TCP throughput and causes network congestion. If you set this parameter to 0, an MTU of 576 bytes is used for all connections that are not to computers on the local subnet.

- ForwardBufferMemory
    - Key: `Tcpip\Parameters`
    - Value type: REG_DWORD - Number of bytes
    - Valid range: network MTU - some reasonable value smaller than 0xFFFFFFFF
    - Default: 74240 (sufficient for fifty 1480-byte packets, rounded to a multiple of 256)
    - Description: This parameter determines how much memory IP allocates to store packet data in the router packet queue. When this buffer space is filled, the router starts to discard packets at random from its queue. Packet queue data buffers are 256 bytes in length. Therefore, the value of this parameter must be a multiple of 256. Multiple buffers are chained together for larger packets. The IP header for a packet is stored separately. This parameter is ignored and no buffers are allocated if the IP router is not enabled.

- IGMPLevel
    - Key: `Tcpip\Parameters`

    - Value type: REG_DWORD - Number
    - Valid range: 0,1,2
    - Default: 2
    - Description: This parameter determines how well the computer supports IP multicasting and participates in the Internet Group Management Protocol. At level 0, the computer provides no multicast support. At level 1, the computer can only send IP multicast packets. At level 2, the computer can send IP multicast packets and fully participate in IGMP to receive multicast packets.

- KeepAliveInterval
    - Key: `Tcpip\Parameters`
    - Value type: REG_DWORD - Time in milliseconds
    - Valid range: 1 - 0xFFFFFFFF
    - Default: 1000 (one second)
    - Description: This parameter determines the interval that separates keepalive retransmissions until a response is received. After a response is received, KeepAliveTime again controls the delay until the next keepalive transmission. The connection is aborted after the number of retransmissions that are specified by TcpMaxDataRetransmissions are unanswered.

- KeepAliveTime
    - Key: `Tcpip\Parameters`
    - Value type: REG_DWORD - Time in milliseconds
    - Valid range: 1 - 0xFFFFFFFF
    - Default: 7,200,000 (two hours)
    - Description: The parameter controls how frequently TCP tries to verify that an idle connection is still intact by sending a keepalive packet. If the remote computer is still reachable and functioning, the remote computer acknowledges the keepalive transmission. By default, keepalive packets are not sent. A program can turn on this feature on a connection.

- MTU
    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
    - Value type: REG_DWORD Number
    - Valid range: 68 - the MTU of the underlying network
    - Default: 0xFFFFFFFF
    - Description: This parameter overrides the default Maximum Transmission Unit (MTU) for a network interface. The MTU is the maximum packet size in bytes that the transport transmits over the underlying network. The size includes the transport header. An IP datagram can span multiple packets. Values larger than the default value for the underlying network cause the transport to use the

network default MTU. Values smaller than 68 cause the transport to use an MTU of 68.

- NumForwardPackets
  - Key: `Tcpip\Parameters`
  - Value type: REG_DWORD Number
  - Valid range: 1 - some reasonable value smaller than 0xFFFFFFFF
  - Default: 50
  - Description: This parameter determines the number of IP packet headers that are allocated for the router packet queue. When all headers are in use, the router begins to discard packets at random from the queue. This value should be at least as large as the ForwardBufferMemory value divided by the maximum IP data size of the networks that are connected to the router. This value must be no larger than the ForwardBufferMemory value divided by 256 because at least 256 bytes of forward buffer memory are used for each packet. The optimal number of forward packets for a particular ForwardBufferMemory size depends on the type of traffic that is carried on the network and will be somewhere between these two values. This parameter is ignored and no headers are allocated if the router is not enabled.

- TcpMaxConnectRetransmissions
  - Key: `Tcpip\Parameters`
  - Value type: REG_DWORD - Number
  - Valid range: 0 - 0xFFFFFFFF
  - Default: 2
  - Description: This parameter determines the number of times that TCP retransmits a connect request (SYN) before aborting the attempt. The retransmission timeout is doubled with each successive retransmission in a particular connect attempt. The initial timeout value is three seconds.

- TcpMaxDataRetransmissions
  - Key: `Tcpip\Parameters`
  - Value type: REG_DWORD - Number
  - Valid range: 0 - 0xFFFFFFFF
  - Default: 5
  - Description: This parameter controls the number of times that TCP retransmits an individual data segment (non-connect segment) before it aborts the connection. The retransmission timeout is doubled with each successive retransmission on a connection. It is reset when responses resume. The base timeout value is dynamically determined by the measured round-trip time on the connection.

- TcpNumConnections
  - Key: `Tcpip\Parameters`
  - Value type: REG_DWORD - Number
  - Valid range: 0 - 0xfffffe
  - Default: 0xfffffe
  - Description: This parameter limits the maximum number of connections that TCP can have open at the same time.

- TcpTimedWaitDelay
  - Key: `Tcpip\Parameters`
  - Value type: REG_DWORD - Time in seconds
  - Valid range: 30-300 (decimal)
  - Default: 0x78 (120 decimal)
  - Description: This parameter determines the time that a connection stays in the TIME_WAIT state when it is closing. As long as a connection is in the TIME_WAIT state, the socket pair cannot be re-used. This is also known as the "2MSL" state. According to RFC793, the value should be two times the maximum segment lifetime on the network. See RFC793 for more information.

    > **Note**
    >
    > In Microsoft Windows 2000, the default value is 240 seconds. For Windows XP and Microsoft Windows Server 2003, the default was changed to 120 seconds for the IPv4 stack to increase performance. The default value for the IPv6 stack is 240 seconds.

- TcpUseRFC1122UrgentPointer
  - Key: `Tcpip\Parameters`
  - Value type: REG_DWORD - Boolean
  - Valid range: 0,1 (False, True)
  - Default: 0 (False)
  - Description: This parameter determines whether TCP uses the RFC 1122 specification for urgent data or the mode that is used by BSD-derived computers. The two mechanisms interpret the urgent pointer in the TCP header and the length of the urgent data differently. They are not interoperable. By default, Windows XP uses the BSD mode.

- TcpWindowSize

- Key: `Tcpip\Parameters`
- Value type: REG_DWORD - Number of bytes
- Valid range: 0 - 0xFFFF
- Default: The smaller of 0xFFFF OR the larger of four times the maximum TCP data size on the network OR 8192 rounded up to an even multiple of the network TCP data size.
- Ethernet default: 8760
- Description: This parameter determines the maximum TCP receive window size of the computer. The receive window specifies the number of bytes a sender can transmit without receiving an acknowledgment. Generally, larger receive windows improve performance over high (delay * bandwidth) networks. For highest efficiency, the receive window must be an even multiple of the TCP Maximum Segment Size (MSS).

TCP/IP parameters that are configurable from the properties of a network connection

The following parameters are created and modified automatically by the connection properties interface through user-supplied information. You do not have to configure them directly in the registry.

- DefaultGateway
  - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
  - Value type: REG_MULTI_SZ - List of dotted decimal IP addresses
  - Valid range: Any set of valid IP addresses
  - Default: None
  - Description: This parameter specifies the list of gateways to route packets that are not destined for a subnet that the computer is directly connected to and that do not have a more specific route. This parameter overrides the DhcpDefaultGateway parameter.

- Domain
  - Key: `Tcpip\Parameters`
  - Value type: REG_SZ - Character string
  - Valid range: Any valid DNS domain name
  - Default: None
  - Description: This parameter specifies the DNS domain name of the computer. It is used by the Windows Sockets interface.

- EnableDhcp

    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
    - Value type: REG_DWORD - Boolean
    - Valid range: 0 or 1 (False or True)
    - Default: 0 (False)
    - Description: If this parameter is set to 1 (True), the DHCP client service tries to use DHCP to configure the first IP interface on the adapter.

- Hostname
    - Key: `Tcpip\Parameters`
    - Value type: REG_SZ - Character string
    - Valid range: Any valid DNS hostname
    - Default: The computer name of the computer
    - Description: This parameter specifies the DNS hostname of the computer that will be returned by the hostname command.

- IPAddress
    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
    - Value type: REG_MULTI_SZ - List of dotted- decimal IP addresses
    - Valid range: Any set of valid IP addresses
    - Default: None
    - Description: This parameter specifies the IP addresses of the IP interfaces to be bound to the adapter. If the first address in the list is 0.0.0.0, the primary interface on the adapter will be configured from DHCP. A computer with more than one IP interface for an adapter is known as "logically multihomed." There must be a valid subnet mask value in the SubnetMask parameter for each IP address that is specified in this parameter.

- IPEnableRouter
    - Key: `Tcpip\Parameters`
    - Value type: REG_DWORD - Boolean
    - Valid range: 0 or 1 (False or True)
    - Default: 0 (False)
    - Description: Setting this parameter to 1 (True) causes the computer to route IP packets between the networks that it is connected to.

- NameServer
    - Key: `Tcpip\Parameters`
    - Value type: REG_SZ - A space delimited list of dotted decimal IP addresses
    - Valid range: Any set of valid IP address
    - Default: None (Blank)
    - Description: This parameter specifies the DNS name servers to be queried by Windows Sockets to resolve names.

- SearchList
  - Key: `Tcpip\Parameters`
  - Value type: REG_SZ - Delimited list of DNS domain name suffixes
  - Valid range: Any set of valid DNS domain name suffixes
  - Default: None
  - Description: This parameter specifies a list of domain name suffixes to append to a name to be resolved by the DNS if resolution of the unadorned name fails. By default, the value of the Domain parameter is appended only. This parameter is used by the Windows Sockets interface.

- SubnetMask
  - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
  - Value type: REG_MULTI_SZ - List of dotted decimal IP addresses
  - Valid range: Any set of valid IP addresses.
  - Default: None
  - Description: This parameter specifies the subnet masks to be used with the IP interfaces bound to the adapter. If the first mask in the list is 0.0.0.0, the primary interface on the adapter will be configured by DHCP. There must be a valid subnet mask value in this parameter for each IP address that is specified in the IPAddress parameter.

Non-configurable TCP/IP parameters

The following parameters are created and used internally by the TCP/IP components. They should never be modified by using Registry Editor. They are listed here for reference only.

- DhcpDefaultGateway
  - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
  - Value type: REG_MULTI_SZ - List of dotted decimal IP addresses
  - Valid range: Any set of valid IP addresses
  - Default: None
  - Description: This parameter specifies the list of default gateways to route packets that are not destined for a subnet that the computer is directly connected to, and that do not have a more specific route. This parameter is written by the DHCP client service, if enabled. This parameter is overridden by a valid DefaultGateway parameter value.

- DhcpIPAddress
  - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
  - Value type: REG_SZ - Dotted decimal IP address

    - Valid range: Any valid IP address
    - Default: None
    - Description: This parameter specifies the DHCP-configured IP address for the interface. If the IPAddress parameter contains a first value other than 0.0.0.0, that value will override this parameter.

- DhcpNameServer
    - Key: `Tcpip\Parameters`
    - Value type: REG_SZ - A space delimited list of dotted decimal IP addresses
    - Valid range: Any set of valid IP address
    - Default: None
    - Description: This parameter specifies the DNS name servers to be queried by Windows Sockets to resolve names. It is written by the DHCP client service, if enabled. The NameServer parameter overrides this parameter.

- DhcpServer
    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
    - Value type: REG_SZ - Dotted decimal IP address
    - Valid range: Any valid IP address
    - Default: None
    - Description: This parameter specifies the IP address of the DHCP server that granted the lease on the IP address in the DhcpIPAddress parameter.

- DhcpSubnetMask
    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
    - Value type: REG_SZ - Dotted decimal IP subnet mask
    - Valid range: Any subnet mask that is valid for the configured IP address
    - Default: None
    - Description: This parameter specifies the DHCP-configured subnet mask for the address that is specified in the DhcpIPAddress parameter.

- IPInterfaceContext
    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
    - Value type: REG_DWORD
    - Valid range: 0 - 0xFFFFFFFF
    - Default: None
    - Description: This parameter is written by the TCP/IP driver for use by the DHCP client service.

- Lease
    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
    - Value type: REG_DWORD - Time in seconds

    - Valid range: 1 - 0xFFFFFFFF
    - Default: None
    - Description: This parameter is used by the DHCP client service to store the time (in seconds) that the lease on the IP address for this adapter is valid for.

- LeaseObtainedTime
    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
    - Value type: REG_DWORD - Absolute time in seconds since midnight of 1/1/70
    - Valid range: 1 - 0xFFFFFFFF
    - Default: None
    - Description: This parameter is used by the DHCP client service to store the time that the lease on the IP address for this adapter obtained.

- LeaseTerminatesTime
    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
    - Value type: REG_DWORD - Absolute time in seconds since midnight of 1/1/70
    - Valid range: 1 - 0xFFFFFFFF
    - Default: None
    - Description: This parameter is used by the DHCP client service to store the time that the lease on the IP address for this adapter expires.

- LLInterface
    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
    - Value type: REG_SZ - NT device name
    - Valid range: A valid NT device name
    - Default: Empty string (Blank)
    - Description: This parameter is used to direct IP to bind to a different link-layer protocol than the built-in ARP module. The value of the parameter is the name of the Windows NT-based device that IP should bind to. This parameter is used in conjunction with the RAS component, for example.

- T1
    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`
    - Value type: REG_DWORD - Absolute time in seconds since midnight of 1/1/70
    - Valid range: 1 - 0xFFFFFFFF
    - Default: None
    - Description: This parameter is used by the DHCP client service to store the time that the service will first try to renew the lease on the IP address for the adapter. To renew the lease, he service contacts the server that granted the lease.

- T2
    - Key: `Tcpip\Parameters\Interfaces\ID for Adapter`

    - Value type: REG_DWORD - Absolute time in seconds since midnight of 1/1/70
    - Valid range: 1 - 0xFFFFFFFF
    - Default: None
    - Description: This parameter is used by the DHCP client service to store the time that the service will try to renew the lease on the IP address for the adapter. To renew the lease, the service broadcasts a renewal request. Time T2 should be reached only if the service was not able to renew the lease with the original server.

All the NBT parameters are registry values that are located under one of two different subkeys of `HKEY_LOCAL_MACHINE\computer\CurrentControlSet\Services`:

- `Netbt\Parameters`
- `Netbt\Parameters\Interfaces\Tcpip_ID for Adapter`

where **ID for Adapter** represents the network adapter that NBT is bound to. The relationship between an Adapter ID and Network Connection can be determined by examining `HKEY_LOCAL_MACHINE\computer\CurrentControlSet\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}\ID for Adapter\Connection`. The Name value in these keys provides the name that is used for a network connection used in the Network Connections folder. Values under the latter keys are specific to each adapter. If the computer is configured through DHCP, a change in parameters takes effect if the command `ipconfig /renew` is issued in a command shell. Otherwise, you must restart the computer for a change in any of these parameters to take effect.

Standard NBT parameters configurable from Registry Editor

The following parameters are installed with default values by the Network tool in Control Panel during the installation of the TCP/IP components. They may be modified by using Registry Editor (Regedit.exe).

- BcastNameQueryCount
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Count
    - Valid range: 1 to 0xFFFF
    - Default: 3
    - Description: This value determines the number of times NetBT broadcasts a query for a particular name without receiving a response.

- BcastQueryTimeout

    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Time in milliseconds
    - Valid range: 100 to 0xFFFFFFFF
    - Default: 0x2ee (750 decimal)
    - Description: This value determines the time interval between successive broadcast name queries for the same name.

- CacheTimeout
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Time in milliseconds
    - Valid range: 60000 to 0xFFFFFFFF
    - Default: 0x927c0 (600000 milliseconds = 10 minutes)
    - Description: This value determines the time interval that names are cached for in the remote name table.

- NameServerPort
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - UDP port number
    - Valid range: 0 - 0xFFFF
    - Default: 0x89
    - Description: This parameter determines the destination port number that NetBT sends packets to that are related to name service, such as name queries and name registrations to WINS. The Microsoft WINS listens on port 0x89. NetBIOS name servers from other vendors can listen on different ports.

- NameSrvQueryCount
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Count
    - Valid range: 0 - 0xFFFF
    - Default: 3
    - Description: This value determines the number of times NetBT sends a query to a WINS server for a specified name without receiving a response.

- NameSrvQueryTimeout
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Time in milliseconds
    - Valid range: 100 - 0xFFFFFFFF
    - Default: 1500 (1.5 seconds)
    - Description: This value determines the time interval between successive name queries to WINS for a particular name.

- SessionKeepAlive

    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Time in milliseconds
    - Valid range: 60,000 - 0xFFFFFFFF
    - Default: 3,600,000 (1 hour)
    - Description: This value determines the time interval between keepalive transmissions on a session. Setting the value to 0xFFFFFFF disables keepalives.

- Size/Small/Medium/Large
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD
    - Valid range: 1, 2, 3 (Small, Medium, Large)
    - Default: 1 (Small)
    - Description: This value determines the size of the name tables that are used to store local and remote names. Generally, Small is adequate. If the computer is acting as a proxy name server, the value is automatically set to Large to increase the size of the name cache hash table. Hash table buckets are sized as follows: Large: 256 Medium: 128 Small: 16

Optional NBT parameters configurable from Registry Editor

These parameters generally do not exist in the registry. They may be created to modify the default behavior of the NetBT protocol driver.

- BroadcastAddress
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Four bytes, little- endian encoded IP address
    - Valid range: 0 - 0xFFFFFFFF
    - Default: The ones-broadcast address for each network.
    - Description: This parameter can be used to force NetBT to use a specific address for all broadcast name-related packets. By default, NetBT uses the ones-broadcast address that is appropriate for each net (that is, for a network of 11.101.0.0 with a subnet mask of 255.255.0.0, the subnet broadcast address would be 11.101.255.255). This parameter would be set, for example, if the network uses the zeros-broadcast address (set by using the UseZeroBroadcast TCP/IP parameter). The appropriate subnet broadcast address would then be 11.101.0.0 in the earlier example. This parameter would then be set to 0x0b650000. This parameter is global and is used on all subnets that NetBT is bound to.

- EnableProxy

    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Boolean
    - Valid range: 0 or 1 (False or True)
    - Default: 0 (False)
    - Description: If this value is set to 1 (True), the computer acts as a proxy name server for the networks that NBT is bound to. A proxy name server answers broadcast queries for names that it has resolved through WINS. With a proxy name server, a network of B-node implementations can connect to servers on other subnets that are registered with WINS.

- EnableProxyRegCheck
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Boolean
    - Valid range: 0 or 1 (False or True)
    - Default: 0 (False)
    - Description: If this parameter is set to 1 (True), the proxy name server sends a negative response to a broadcast name registration if the name is already registered with WINS or is in the proxy's local name cache with a different IP address. The hazard of enabling this feature is that it prevents a computer from changing its IP address as long as WINS has a mapping for the name. Therefore, it is disabled by default.

- InitialRefreshT.O.
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Time in milliseconds
    - Valid range: 960000 - 0xFFFFFFF
    - Default: 960000 (16 minutes)
    - Description: This parameter specifies the initial update timeout used by NBT during name registration. NBT tries to contact the WINS servers at 1/8th of this time interval when it is first registering names. When it receives a successful registration response, that response contains the new update interval to use.

- LmhostsTimeout
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Time in milliseconds
    - Valid range: 1000 - 0xFFFFFFFF
    - Default: 6000 (6 seconds)
    - Description: This parameter specifies the timeout value for LMHOSTS and DNS name queries. The timer has a granularity of the timeout value. Therefore, the actual timeout might be as much as two times the value.

- MaxDgramBuffering

    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Count of bytes
    - Valid range: 0 - 0xFFFFFFFF
    - Default: 0x20000 (128 Kb)
    - Description: This parameter specifies the maximum memory that NetBT dynamically allocates for all outstanding datagram sends. After this limit is reached, additional sends will fail because the available resources are not sufficient resources.

- NodeType
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Number
    - Valid range: 1,2,4,8 (B-node, P-node, M-node, H-node)
    - Default: 1 or 8 based on the WINS server configuration
    - Description: This parameter determines what methods NetBT uses to register and resolve names. A B-node computer uses broadcasts. A P-node computer uses only point- to-point name queries to a name server (WINS). An M-node computer broadcasts first, and then queries the name server. An H-node computer queries the name server first, and then broadcasts. Resolution through LMHOSTS or DNS follows these methods. If this key is present, it will override the DhcpNodeType key. If neither key is present, the computer uses B-node if there are no WINS servers configured for the network. The computer uses H-node if there is at least one WINS server configured.

- RandomAdapter
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Boolean
    - Valid range: 0 or 1 (False or True)
    - Default: 0 (False)
    - Description: This parameter applies to a multihomed host only. If it is set to 1 (True), NetBT will randomly select the IP address to put in a name query response from all its bound interfaces. Frequently, the response contains the address of the interface that the query arrived on. This feature would be used by a server with two interfaces on the same network for load balancing.

- RefreshOpCode
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Number
    - Valid range: 8, 9
    - Default: 8

    - Description: This parameter forces NetBT to use a specific opcode in name update packets. The specification for the NetBT protocol is somewhat ambiguous in this area. Although the default of 8 that is used by Microsoft implementations appears to be the intended value, some other implementations, such as those by Ungermann-Bass, use the value 9. Two implementations must use the same opcode to interoperate.

- SingleResponse
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Boolean
    - Valid range: 0 or 1 (False or True)
    - Default: 0 (False)
    - Description: This parameter applies to a multihomed host only. If this parameter is set to 1 (True), NBT will only supply an IP address from one of its bound interfaces in name query responses. By default, the addresses of all bound interfaces are included.

- WinsDownTimeout
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Time in milliseconds
    - Valid range: 1000 - 0xFFFFFFFF
    - Default: 15,000 (15 seconds)
    - Description: This parameter determines the time that NBT waits before again trying to use WINS after it does not contact any WINS server. With this feature, computers that are temporarily disconnected from the network can proceed through boot processing without waiting to time out each WINS name registration or query individually.

NBT parameters configurable from the Connection Properties

The following parameters can be set through the Connection Properties from the Network Connections folder. You do not have to configure them directly.

- EnableDns
    - Key: `Netbt\Parameters`
    - Value type: REG_DWORD - Boolean
    - Valid range: 0 or 1 (False or True)
    - Default: 0 (False)
    - Description: If this value is set to 1 (True), NBT queries the DNS for names that cannot be resolved by WINS, broadcast, or the LMHOSTS file.

- EnableLmhosts
  - Key: `Netbt\Parameters`
  - Value type: REG_DWORD - Boolean
  - Valid range: 0 or 1 (False or True)
  - Default: 1 (True)
  - Description: If this value is set to 1 (True), NBT searches the LMHOSTS file, if it exists, for names that cannot be resolved by WINS or broadcast. By default, there is no LMHOSTS file database directory (specified by `Tcpip\Parameters\DatabasePath`). Therefore, NBT takes no action. This value is written by the Advanced TCP/IP configuration under the Network tool in Control Panel.

- NameServer
  - Key: `Netbt\Parameters\Interfaces\Tcpip_ID for Adapter`
  - Value type: REG_SZ - Dotted decimal IP address (for example,11.101.1.200)
  - Valid range: Any valid IP address
  - Default: blank (no address)
  - Description: This parameter specifies the IP address of the primary WINS server. If this parameter contains a valid value, it overrides the DHCP parameter of the same name.

- NameServerBackup
  - Key: `Netbt\Parameters\Interfaces\Tcpip_ID for Adapter`
  - Value type: REG_SZ - Dotted decimal IP address (for example, 11.101.1.200)
  - Valid range: Any valid IP address.
  - Default: blank (no address)
  - Description: This parameter specifies the IP address of the backup WINS server. If this parameter contains a valid value, it overrides the DHCP parameter of the same name.

- ScopeId
  - Key: `Netbt\Parameters`
  - Value type: REG_SZ - Character string
  - Valid range: Any valid DNS domain name consisting of two dot-separated parts, or a "*".
  - Default: None
  - Description: This parameter specifies the NetBIOS name scope for the node. This value must not start with a period. If this parameter contains a valid value, it will override the DHCP parameter of the same name. A blank value (empty string) will be ignored. Setting this parameter to the value "*" indicates a null scope and will override the DHCP parameter.

Non-configurable NBT parameters

The following parameters are created and used internally by the NetBT components. They should never be modified by using Registry Editor. They are listed here for reference only.

- DhcpNameServer
  - Key: `Netbt\Parameters\Interfaces\Tcpip_ID for Adapter`
  - Value type: REG_SZ - Dotted decimal IP address (for example, 11.101.1.200)
  - Valid range: Any valid IP address
  - Default: None
  - Description: This parameter specifies the IP address of the primary WINS server. It is written by the DHCP client service, if enabled. A valid NameServer value will override this parameter.

- DhcpNameServerBackup
  - Key: `Netbt\Parameters\Interfaces\Tcpip_ID for Adapter`
  - Value type: REG_SZ - Dotted decimal IP address (for example, 11.101.1.200)
  - Valid range: Any valid IP address
  - Default: None
  - Description: This parameter specifies the IP address of the backup WINS server. It is written by the DHCP client service, if enabled. A valid BackupNameServer value will override this parameter.

- DhcpNodeType
  - Key: `Netbt\Parameters`
  - Value type: REG_DWORD - Number
  - Valid range: 1 - 8
  - Default: 1
  - Description: This parameter specifies the NBT node type. It is written by the DHCP client service, if enabled. A valid NodeType value will override this parameter. See the entry for NodeType for a complete description.

- DhcpScopeId
  - Key: `Netbt\Parameters`
  - Value type: REG_SZ - Character string
  - Valid range: a dot-separated name string such as `microsoft.com`
  - Default: None
  - Description: This parameter specifies the NetBIOS name scope for the node. It is written by the DHCP client service, if enabled. This value must not start with a period. See the entry for ScopeId for more information.

- NbProvider
  - Key: `Netbt\Parameters`
  - Value type: REG_SZ - Character string
  - Valid Range: _tcp
  - Default: _tcp
  - Description: This parameter is used internally by the RPC component. The default value should not be changed.

- TransportBindName
  - Key: `Netbt\Parameters`
  - Value type: REG_SZ - Character string
  - Valid range: N/A
  - Default: \Device\
  - Description: This parameter is used internally during product development. The default value should not be changed.

How to troubleshoot missing network connections icons in Windows Server 2003 and in Windows XP

Article • 09/23/2021 • 15 minutes to read

This article describes how to troubleshoot missing network connections icons in Windows Server 2003 and in Windows XP.

Applies to: Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 825826

Introduction

This article describes general step-by-step methods and advanced troubleshooting methods that you can use to restore missing network and dial-up connections icons on a computer that runs Windows XP or Windows Server 2003. However, despite the missing icons, networking continues to function correctly. Because missing network icons can be a symptom of several issues, it is difficult to say what is causing your particular problem until you examine it a bit. We'll ask you some questions. Then, based on your answers, we'll determine which of these methods that you should try first.

This article provides self-help steps for a beginning to intermediate computer user. The "Advanced troubleshooting" section is designed for the advanced computer user. You may find it easier to follow the steps if you print this article first.

Symptoms

When you click **Start**, point to and click **Control Panel**, and then double-click **Network Connections**, or if you right-click **My Network Places** on the desktop and then click **Properties**, you do not see all network icons. Or, you may experience problems with the **Network Connections** window.

To know which method you should try first to resolve your problem, review the following four cases to determine which symptoms match your situation.

Case 1: All or some of the network icons are missing

- The **LAN or High-Speed Internet** connection icon is missing.

- The **Dial-up Connection** icons are missing.
- The **New Connection Wizard** icon is missing.
- Only the **New Connection Wizard** icon appears. Or, one or more dial-up connections also appear.
- If you click the **Advanced** menu and then click **Advanced Settings**, only the **Remote Access connections** entry appears in the **Connections** list.

If this case describes your situation, you should first try Method 1 in the "General troubleshooting" section to let Windows automatically detect and install network adapters.

Case 2: Only the "Dial-up Connection" icons are missing

If this case describes your situation, you should first try Method 5 in the "General troubleshooting methods" section to add a generic standard modem.

Case 3: The Network Connections window stops responding (hangs) or closes immediately after you select a network connection and then click "Properties"

If this case describes your situation, try Method 4 in the "Advanced troubleshooting" section to reconstruct the Config entry of the Network subkey. If you do not feel comfortable performing advanced troubleshooting, you may want to ask someone for help or contact support.

Case 4: The network icon disappears only after you manually connect to the network

If this describes your situation, try Method 3 in the "Advanced troubleshooting" section to use the Group Policy Results tool or the Group Policy Management Console to diagnose and resolve the problem. If you do not feel comfortable performing advanced troubleshooting, you may want to ask someone for help or contact support.

General troubleshooting

Method 1: Let Windows automatically detect and install network adapters

Windows can automatically detect and install the correct network adapters for you. It will also correct any corrupted registry entries on the network adapter.

To direct Windows to automatically detect and install network adapters for you, follow these steps:

1. Right-click **My Computer**, and then click **Properties**.
2. Click the **Hardware** tab, and then click **Device Manager**.
3. To see a list of installed network adapters, expand **Network adapter(s)**. Click to locate the network adapter, and then click **Uninstall**.
4. Restart the computer, and then let the system automatically detect and install the network adapter drivers.

Check to see whether your networking icons appear. If this method worked for you, you are finished with this article. However, you might want to read the "Prevention tips" section to learn how you can avoid this problem in the future.

If this method did not work for you, try Method 2.

Method 2: Verify network settings and services

Network settings such as adapter settings, services settings, the logon setting, the desktop interaction setting, and networking services settings enable you to use your computer to connect to a network. If these settings are incorrect, network connectivity issues can occur.

To verify network settings and services, follow these steps:

1. Verify that the correct network adapter is selected. A network adapter is a device that enables you to connect a computer to a network. It is also known as a network interface card (NIC).
   a. Right-click **My Computer**, click **Properties**, click the **Hardware** tab, and then click **Device Manager**.
   b. Double-click **Network adapters**, and then verify that the correct network adapter name is selected. If you do not know the name of your network adapter, don't worry. For now, just make sure that an adapter is selected.
   c. Double-click the network adapter, and then verify that the "This device is working properly" message appears in the **Device status** box on the **General** tab. If you do not see this message, click **Troubleshoot**, and follow the directions.
   d. After you confirm that the correct network adapter is selected and is working properly, you can close all the open dialog boxes.

2. Verify that the necessary services are started. The Services settings direct the system to stop, start, and administer system services.
   a. Right-click **My Computer**, and then click **Manage**.
   b. Double-click **Services and Applications**, and then click **Services**.
   c. In the right pane, look at the **Status** column. You may need to expand the box so that you can see all the columns. Make sure that the following services are started:

      - Remote procedure call (RPC)

        > ⓘ **Note**
        >
        > This service must be started before other services can take effect.

      - Network Connections

        > ⓘ **Note**
        >
        > This service can only start if the RPC service is active.

      - Plug and Play
      - COM+ Event System

        > ⓘ **Note**
        >
        > This service can only start if the RPC service is active.

      - Remote Access Connection Manager

        > ⓘ **Note**
        >
        > This service can only start if Telephony service is active.

      - Telephony

        > ⓘ **Note**
        >
        > This service can only start if the RPC service and the PnP Service are active.

   d. To start a service, right-click the service name, and then click **Start**.

e. Do not close the **Computer Management** box because you will need to check additional settings in the remaining steps.

3. Verify the logon setting.
   a. In the right pane, double-click **COM+ Event System service**.
   b. Click the **Log On** tab.
   c. Under **Log on as**, verify that the **Local System account** is selected.
4. Verify the desktop interaction setting.
   a. Double-click the **Network Connections** service.
   b. Click the **Log On** tab.
   c. Under **Log on as**, verify that the **Local System Account** option is selected.
   d. Verify that the **Allow service to interact with desktop** check box is selected, and then click **OK**.
   e. Close the **Computer Management** box.
5. Verify the network services setting.
   a. Click **Start**, and then click **Control Panel**.
   b. Double-click **Add or Remove Programs**.
   c. Click **Add/Remove Windows Components**.
   d. Scroll down and then click **Networking Services**, and then click **Details**. Verify that **Simple TCP/IP Services** is turned on, and then click **OK**.
   e. Close all the open dialog boxes.
6. Verify that the network DLL files are registered correctly. DLL files are small files that include a library of functions and data that can be shared across multiple applications.

   a. Click **Start**, and then click **Run**.

   b. In the **Run** box, type *cmd.exe*, and then click **OK**.

   c. Type the following lines. Press ENTER after you type each line. This command text is difficult to type. Be sure that you type it exactly as it appears below. Or you may find it easier to copy and paste the text instead. Click **OK** when the **RegSvr32** dialog box appears for each command.

   ```
   Console

   regsvr32 netshell.dll
   regsvr32 netcfgx.dll
   regsvr32 netman.dll
   ```

   d. Restart the computer. Check to see whether your networking icons appear. If this method worked for you, you are finished with this article. However, you might want to read the "Prevention tips" section to avoid this problem in the future.

If this method did not work for you, try Method 3.

Method 3: Determine if a third-party driver is incompatible with the latest Windows Service Pack

A driver is software that allows your computer to communicate with hardware or devices. If you have an out-of-date driver installed, it may not be compatible with the latest Windows Service Pack. You can correct this incompatibility by checking to see if a driver update is available.

To check to see if a new network adapter driver is available, follow these steps:

1. Click **Start**, point to **All Programs**, and then click **Windows Update**.
2. Click **Custom Install**, and then click **Select optional hardware update**.
3. Look for the network adapter name, and then install any available hardware updates. If you do not find the driver listed, you may want to check the manufacturer's Web site for more information.
4. Restart the computer if you were prompted to install hardware updates. Check to see whether your networking icons appear. If this method worked for you, you are finished with this article. However, you might want to read the "Prevention tips" section to avoid this problem in the future.

If this method did not work for you, you can try Method 4.

Method 4: Use the Dcomcnfg.exe utility to reset the "Default Impersonation Level" setting

This setting tells the computer how you want it to authenticate who can connect to a network. This method sounds more intimidating than what it really is. The DCOM Config utility has a point-and-click interface, and you just need to follow the steps, and it will do the "dirty" work for you.

Before you get started, you will need to make sure that you are logged on to the computer by using an administrator account. With an administrator account, you can make changes to your computer that you cannot make with any other account, such as a standard account. If you are using your own computer, chances are that you are logged on with an administrator account.

If you are unsure whether you have administrative user rights, follow these steps. Otherwise, go to step 1.

1. Open the **Date and Time Properties** dialog box.

a. Click **Start**, and then click **Run**.
b. In the **Open** box, type *timedate.cpl*, and then press ENTER.

2. Now determine whether you are logged on with an administrator account.

    - If the **Date and Time Properties** dialog box opened after you performed step 1, you are logged on as a computer administrator. Close the **Date and Time Properties** dialog box, and then continue with this method.
    - If you received the following message, you are not logged on as an administrator:

        > You do not have the proper privilege level to change the system time.

To continue with this task, you must first log off, and then log back on to Windows by using a computer administrator account. If you do not know how to log back on to Windows by using a computer administrator account, you might have to ask someone for help. If this computer is part of a network at work, you can ask the system administrator for help. However, if you have to perform this task on a home computer that is not part of a network, you must know the password for an administrator account on your computer.

Unfortunately, if you do not know the password for any administrator account on your computer, this content is unable to help you any further. You may want to contact support. See "Next steps" for information about how to contact support.

To run the Dcomcnfg.exe utility to rest the **Default Impersonation Level** setting, follow these steps:

1. Click **Start**, and then click **Run**.
2. Type *dcomcnfg*, and then click **OK**.
3. In **Component Services**, click **Computers**, right-click the computer whose machine-wide impersonation level that you want to modify (for example, My Computer), and then click **Properties**.
4. Click the **Default Properties** tab, and then click to select the **Enable Distributed COM on this computer** check box for this computer.
5. Click the down arrow in the **Default Impersonation Level** box, and then click any setting other than **Anonymous**, and then click **OK**.

The new machine-wide impersonation level is available the next time that you start a program. Programs that are currently running are not affected until you restart them.

Check to see whether your networking icons appear. If this method worked for you, you are finished with this article.

If this method did not work for you, you can try Method 5.

Method 5: If only the Dial-up Connection icons are missing, temporarily add a new modem

Try adding a standard modem. Often, just the process of adding a new modem causes the connection icons to reappear. To add a standard modem, complete these steps:

1. Click **Start**, and then click **Control Panel**.
2. If it is not already selected, click **Switch to Classic View**. This option appears on the left side of **Control Panel**.
3. Double-click **Phone and Modem Options**.
4. Click **Modems**, and then click **Add**. The **Add Hardware Wizard** starts.
5. Click to select the **Don't detect my modem I will select it from a list** check box, and then click **Next**.
6. Select a standard modem from the list on the left, and then click **Next**. When the icons reappear, you can safely delete the modem that you added in this procedure.

Advanced troubleshooting

If you are still experiencing the missing icons problem, you can try the advanced methods. If you are not comfortable with advanced troubleshooting, you might want to contact Support. For information about how to contact support, see the "Next steps" section.

We recommend the following advanced troubleshooting methods for advanced users:

- Method 1: Verify that all Windows Protected Files in the System 32 folder are intact
- Method 2: Remove third-party network adapter management software
- Method 3: Use the Group Policy Results tool to see which Group Policy objects are applied
- Method 4: Reset the network connections
- Method 5: Verify that the registry keys are intact and correct
- Method 6: Check for nonpresent, ghosted, or hidden network adapters
- Method 7: Remove all the AutoDiscovery/AutoPurge (ADAP) information from the registry and reset the state of each performance library

Method 1: Verify that all Windows Protected Files in the System 32 folder are intact

System File Checker enables an administrator to scan all protected files to verify their versions. If System File Checker discovers that a protected file has been overwritten, it retrieves the correct version of the file from the cache folder (%Systemroot%\System32\Dllcache) or from the Windows installation source files, and then it replaces the incorrect file. System File Checker also checks and repopulates the cache folder. You must be logged on as an administrator or as a member of the Administrators group to run System File Checker.

To run System File Checker, open a command prompt, type `sfc /purgecache`, and then press ENTER. The Window File Checker starts.

For more information about how to use the Windows File Protection feature, review the following Microsoft Knowledge Base article:
222193 Description of the Windows File Protection feature

Method 2: Remove third-party network adapter management software

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Temporarily remove any teaming software. The following combination is known to be incompatible: Dual-Port Intel Pro 100+ Server Adapter with Intel Teaming Software running an SNMP component.

For an updated version of the Intel SNMP agent (Ilansnmp.dll) and for more information, contact the network adapter manufacturer or the third-party software vendor.

Method 3: Use the Group Policy Results tool to see which Group Policy objects are applied

If the icon is being deleted only after you manually connect to the network, follow these steps:

1. Restart the computer while it is not connected to the network to see whether a Group Policy Object (GPO) is being downloaded.
2. Start the Group Policy Results tool to find out which GPOs are applied.
3. Click **Start**, click **Run**, type *gpedit.msc*, and press ENTER.
4. Locate and open **Group policy/User Configuration/Windows Settings/Internet Explorer Maintenance/Connection/Connection Settings/**.

Method 4: Reset the network connections

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:
> 322756 How to back up and restore the registry in Windows

If the Network Connections window starts to open, but then closes immediately or "hangs," complete these steps:

1. Click **Start**, click **Run**, type *regedit*, and then press ENTER.
2. Locate and then click the following registry subkey:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Network`
3. Right-click this subkey, click **Export**, and then save the selected branch in a file.
4. Click the Network subkey again, and then delete the Config entry. Do not delete the Network subkey. The Config entry will be reconstructed when you restart the computer.
5. Restart the computer. You may have to manually turn off the computer.

Method 5: Verify that the registry keys are intact and correct

To verify that the registry keys are intact and correct, complete these steps:

1. Click **Start**, click **Run**, type *regedit*, and then press ENTER.
2. Locate and then click the following registry subkey: `HKEY_CLASSES_ROOT\Interface\{0000010C-0000-0000-C000-00000000046}`

   Verify that the subkeys NumMethods and ProxyStubClsid32 exist and that their values are correct. If these registry subkeys do not exist, create them.

Method 6: Check for nonpresent, ghosted, or hidden network adapters

To uninstall the ghosted network adapter from the registry, complete these steps:

1. Click **Start**, click **Run**, type *cmd.exe*, and then press ENTER.
2. Type `set devmgr_show_nonpresent_devices=1`, and then press ENTER.
3. Type `Start DEVMGMT.MSC`, and then press ENTER.
4. Click **View**, and then click **Show Hidden Devices**.
5. Expand the **Network adapters** tree.
6. Right-click the dimmed network adapter, and then click **Uninstall**.

Method 7: Remove all the AutoDiscovery/AutoPurge (ADAP) information from the registry and reset the state of each performance library

To do this, open a command prompt, type `winmgmt / clearadap`, and then press ENTER.

Next steps

If you were unable to complete the steps in this article to restore your network icons, you might have to ask someone for help or contact support.

To view Microsoft support options, visit the following Microsoft Web site: Contact us

Prevention tips

To prevent these problems in the future, try to keep your computer up-to-date. Always make sure that you have the most recent drivers installed on the computer. To do this, you can use Windows Update to install the latest drivers. For more information, visit the following Microsoft Web site: https://update.microsoft.com

Unwanted wake-up events occur when you enable the Wake On LAN feature

Article • 09/23/2021 • 3 minutes to read

This article explains why unwanted wake-up events occur when you enable the Wake On LAN (WOL) functionality in Windows 7 and in Windows Vista, and describes how to configure the computer to wake only in response to a Magic Packet.

Applies to: Windows 7 Service Pack 1
Original KB number: 941145

Introduction

In Windows 7 and in Windows Vista, the WOL feature can wake a remote computer from a power-saving state such as sleep. When you enable WOL, the network adapter continues listening to the network when the computer is asleep. WOL wakes the computer if it receives a special data packet.

One kind of special data packet contains a wake-up pattern. By default, Windows 7 and Windows Vista listen for the following packets when you enable WOL:

- A directed packet to the MAC address of the network adapter
- A NetBIOS name resolution broadcast for the local computer name
- An Address Resolution Protocol (ARP) packet for the IPv4 address of the network adapter
- An IPv6 Neighbor Discovery packet for the network adapter's solicited-node multicast addressA Magic Packet can also wake a remote computer.

A Magic Packet is a standard wake-up frame that targets a specific network interface.

In most cases, a wake-up pattern or a Magic Packet enables remote access to a computer that is in a power-saving state. However, some networking protocols use these packets for other purposes. For example, routers use ARP packets to periodically confirm the presence of a computer. Such protocols do not use these packets to wake computers. However, in some networks, network traffic may wake up a remote computer by mistake. These unwanted wake-up events may occur in especially noisy environments such as enterprise networks. Therefore, by default, WOL is disabled in Windows 7 and in Windows Vista.

More information

WOL can be an effective way to conserve power while keeping a computer reachable on the network.

However, unwanted wake events may occur after you enable WOL. For example, the computer may wake up soon after it enters a power-saving state. One cause may be that the network environment generates wake-up patterns too frequently. In this situation, we strongly recommend that you configure the computer to wake only in response to Magic Packets. Magic Packets are especially designed to wake up a computer from a power-saving state. Also, because a Magic Packet is specific to the MAC address of a network adapter, a Magic Packet is unlikely to be sent accidentally.

To configure Windows 7 in this manner, follow these steps:

1. Click **Start**, type *Network and Sharing Center* in the **Start Search** box, and then press Enter.
2. On the **Tasks** bar, click **Change adapter settings**.
3. Right-click the network adapter that you want to configure, and then click **Properties**. For example, right-click **Local Area Connection**, and then click **Properties**.
4. If you are prompted for an administrator password or for confirmation, type the password or provide confirmation.
5. Click **Configure**.
6. If the network adapter supports WOL, click to select the **Allow this device to wake the computer** check box on the **Power Management** tab, select the **Only allow a magic packet to wake the computer** check box, and then click **OK**.

To configure Windows Vista in this manner, follow these steps:

1. Click **Start**, type Network and Sharing Center in the **Start Search** box, and then press Enter.
2. On the **Tasks** bar, click **Manage network connections**.
3. Right-click the network adapter that you want to configure, and then click **Properties**. For example, right-click **Local Area Connection**, and then click **Properties**.
4. If you are prompted for an administrator password or for confirmation, type the password or provide confirmation.
5. Click **Configure**.
6. If the network adapter supports WOL, select the **Allow this device to wake the computer** check box on the **Power Management** tab, select the **Only allow management stations to wake the computer** check box, and then click **OK**.

You may also have to enable BIOS settings to enable WOL. The specific BIOS settings depend on the manufacturer of the computer.

Use Telnet to test port 3389 functionality

Article • 09/23/2021 • 2 minutes to read

This article describes how to use Telnet to test port 3389 functionality.

Applies to: Windows 10 - all editions *Original KB number:* 187628

Summary

Terminal Server Clients use TCP port 3389 to communicate with Terminal Server. A common problem in a WAN environment is that a firewall or other network filter prevents connectivity with this port. You can run a simple troubleshooting test to make sure the Client can connect to the port. Just try to telnet to the port from the Client.

Test the functionality of port 3389 by using Telnet

To test the functionality of port 3389, use this command from the Client:

```
Console

Telnet tserv 3389
```

where "tserv" is the host name of your Terminal Server.

If telnet is successful, you simply receive the telnet screen and a cursor. On the Terminal Server, Terminal Server Administration will show a blue computer icon with no other information. The Telnet connection will also consume an idle session.

The Terminal Server should disconnect the connection after a few minutes. Or, you can disconnect using Telnet.

This test tells you that you can connect over the port.

Why does Telnet reports that you cannot connect?

If Telnet reports that you cannot connect, there are several possible reasons:

1. If you can connect by replacing "tserv" with the Terminal Server's IP address but not the host name, you may have a DNS or WINS resolution problem.
2. If you can connect when "tserv" is the host name, but cannot connect when "tserv" is the computer name, then you may have a NetBIOS name resolution issue with WINS or an LMHOSTS file.
3. If you cannot connect when "tserv" is the IP address, the host name, or the computer name, then it is likely that port 3389 is blocked somewhere in your WAN.

10060 Connection timed out error with proxy server or ISA Server on slow link

Article • 09/23/2021 • 2 minutes to read

This article provides help to fix Winsock timeout errors that occur on slow, congested, or high latency Internet links with Microsoft Proxy Server or ISA Server.

Applies to: Windows 10 - all editions
Original KB number: 191143

Symptoms

Winsock timeout errors may occur on slow, congested, or high latency Internet links with Microsoft Proxy Server or ISA Server. The following Winsock error Message appears on the client Web browser:

> Proxy Reports:
> 10060 Connection timed out
>
> The Web server specified in your URL could not be contacted. Please check your URL or try your request again.

> **Note**
>
> A timeout error may also occur when connecting to an Internet server that does not exist or if there is more than one default gateway on the Proxy Server computer.

Resolution

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

Adjusting the following TCP/IP setting by adding a subkey in the registry should reduce the number of timeouts by allowing more time for the connection to complete. This setting is not present in the registry by default.

1. Start Registry Editor (Regedt32.exe) and go to the following subkey:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

2. On the **Edit** menu, click **Add Value**, and then add the following information:

   - Value name: TcpMaxDataRetransmissions
   - Value type: REG_DWORD - Number
   - Valid range: 0 - 0xFFFFFFFF
   - Default value: 5 Decimal
   - New value: 10 Decimal

3. Click **OK**, and then quit Registry Editor.

4. Reboot after registry change has been made.

More information

The TcpMaxDataRetransmissions parameter controls the number of times TCP retransmits an individual data segment (non-connect segment) before ending the connection. The retransmission timeout is doubled with each successive retransmission on a connection. It is reset when responses resume. The base timeout value is dynamically determined by the measured round-trip time on the connection.

The default value for this registry entry is 5; double this value to 10 (Decimal) (see step 2 above). If connection timeouts still occur, try doubling the value again to 20 (Decimal).

> ⓘ **Note**
>
> This registry entry may only reduce the number of connection timeout errors that occur. Changes to your Internet connection or router may have to be made to completely resolve the problem.

Using authenticated proxy servers together with Windows 8

Article • 09/23/2021 • 2 minutes to read

This article provides help to solve an issue that occurs when you use apps that connect to the Internet if you use an Internet proxy server that requires authentication.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2778122

Symptoms

If you use an Internet proxy server that requires authentication, you may encounter problems when you use apps that connect to the Internet.

Proxy servers that require authentication either require a username and password to access the Internet or authenticate users by using their current domain credentials.

Depending on your proxy configuration, you may encounter one of the following problems when you use Microsoft Store apps:

- You cannot install updates that are available in the Microsoft Store, and you may receive one of the following error messages:
  - > This app wasn't installed - view details.
  - > Something happened and this app couldn't be installed. Try again. Error code: 0x8024401c
- You cannot install new apps and may receive one of the following error messages:
  - > Your purchase couldnt be completed. Something happened and your purchase cant be completed.
  - > Something happened and this app couldn't be installed. Try again. Error code: 0x8024401c
- When you start the Microsoft Store app, you may receive the following error message:

    - > Your network proxy doesn't work with the Microsoft Store. Contact your system administrator for more information.

- Apps that are included with Windows 8 may indicate that you are not connected to the Internet. If you installed other apps from the Microsoft Store while you were connected to a different network, those apps may also indicate that you are not connected to the Internet. The apps may display one of the following error messages:
    - > There was a problem signing you in.
    - > You are not connected to the Internet.
- Live Tiles for some apps may not update their content or may never show live content.
- Windows Update may not check for updates or download updates, and you receive error code 8024401C or the following error message:
    - > There was a problem checking for updates.

Resolution

The issues that are discussed in this article are resolved in Windows 8.1 and Windows Server 2012 R2.

More information

If you are using Windows 8 or Windows Server 2012, you can reduce the effect of these issues by enabling unauthenticated access through the proxy server. We recommend that you enable unauthenticated access only for connections to URL addresses that are used by each app that has a problem. Some proxy servers may suggest that you create an allow list of URL addresses.

To resolve these issues as they relate to using Microsoft Store apps or to using Microsoft apps that are included with Windows 8 or Windows Update, you can include the following addresses in an allow list on the proxy server and enable HTTP and HTTPS access to them:

- login.live.com
- account.live.com

- clientconfig.passport.net
- wustat.windows.com
- *.windowsupdate.com
- *.wns.windows.com
- *.hotmail.com
- *.outlook.com
- *.microsoft.com
- *.msftncsi.com/ncsi.txt

To resolve these issues for other apps, you may have to contact the application vendor for information about the URL addresses that you should include in your allow list.

You can't access a WebDAV Web folder from a Windows-based client computer

Article • 09/23/2021 • 3 minutes to read

This article provides help to solve an issue where you can't access a Web Distributed Authoring and Versioning (WebDAV) Web folder from a Windows-based client computer.

Applies to: Windows 10 - all editions, Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 912152

Symptoms

You can't access a WebDAV Web folder from a Windows-based client computer. When you try to do this, you may experience the following symptoms:

- When you use a Universal Naming Convention (UNC) path to access the Web folder, you receive an error message that is similar to the following:

  > \\server\webfolder\folder is not accessible. You might not have permission to use this network resource.
  > Contact the administrator of this server to find out if you have access permissions.
  >
  > A device attached to the system is not functioning.
  >
  > error 31 = ERROR_GEN_FAILURE

- When you map a driver letter to access the Web folder, you receive an error message that is similar to the following:

  > Disk is not formatted
  >
  > Windows cannot read from this disk. The disk might be corrupted, or it could be using a format that is not compatible with Windows.

- When you try to enumerate the Web folder at a command prompt, you receive the following error message:

  > File Not Found

Additionally, every time that you try to access the Web folder, memory consumption increases for the Svchost.exe process that contains the WebClient service. This increase may be approximately 20 megabytes (MB) for every 20,000 files in the Web folder. The memory is not released when you stop the WebClient service. The memory is released only if the computer is restarted.

Cause

This problem may occur if all the following conditions are true:

- The client computer is running one of the following configurations:
  - Windows XP with Service Pack 1 (SP1) and security update 896426
  - Windows XP with Service Pack 2 (SP2)
  - Windows XP Professional x64 Edition
  - Windows 7
  - Windows 8
  - Windows 8.1
- The WebDAV folder contains many files. For example, the folder contains 20,000 or more files. By default, Windows XP will enumerate approximately 1,000 files in one Web folder. This number is based on the default setting for the following registry subkey:
  - Path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters\`
  - Value: FileAttributesLimitInBytes
  - Data Type: DWORD
  - Default Value: 1,000,000 decimal (1 MB)
  - Description: This registry subkey determines the maximum collective size of all file attributes in one folder that is allowed by the WebDAV redirector. This attribute limit covers all the PROPFIND and PROPPATCH responses.

The problem occurs because the size of all the file attributes that are returned by the WebDAV server is much larger than what is expected. By default, this size is limited to 1 MB. This limit is for security reasons. For more information, see Folder copy error message when downloading a file that is larger than 50000000 bytes from a Web folder.

Workaround

> **Important**

This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

To work around this problem, add a DWORD entry that is named **FileAttributesLimitInBytes** to the following registry subkey:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters\
```

Configure the **FileAttributesLimitInBytes** registry value to the size that you want, and then restart the WebClient service. To do this, follow these steps:

1. Click **Start**, click **Run**, type *regedit*, and then click **OK**.
2. Locate and then click the following registry subkey:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters\
   ```

3. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
4. Type **FileAttributesLimitInBytes** for the name of the DWORD, and then press ENTER.
5. Right-click **FileAttributesLimitInBytes**, and then click **Modify**.
6. In the **Value data** box, type the value that you want to use, and then click **OK**. For example, if the Web folder contains 20,000 files, type *20000000* in the **Value data** box.

   > **Note**
   >
   > If the default value is 1,000,000 (1 MB), Windows will enumerate a maximum of approximately 1,000 files in one folder. The actual maximum number of files may vary, depending on the number of file attributes or file properties. By default, the WebClient service does not ask for specific WebDAV properties. Therefore, the server returns all file attributes. The Microsoft Office-integrated Webfolders redirector does ask for specific WebDAV properties.

7. Exit Registry Editor.
8. Stop and then restart the WebClient service. To do this, follow these steps:

a. Click **Start**, click **Run**, type *cmd*, and then click **OK**.

b. Type the following commands, and then press ENTER after each command:

Console

```
net stop webclient
net start webclient
```

Windows 7 can't automatically reconnect a DAV share when Basic Authentication is used

Article • 09/23/2021 • 3 minutes to read

This article describes a by-design behavior where Windows 7 can't automatically reconnect a DAV share when Basic Authentication is used.

Applies to: Windows 7 Service Pack 1
Original KB number: 2673544

Symptoms

Consider the following scenario on a Windows 7-based computer:

- You used the Map Network Drive wizard or the Add Network Location wizard to connect a WebDav share or folder.
- Basic Authentication is used for this resource.

> **Note**
>
> Basic Authentication is often used for connections to third-party DAV servers, such as Apache, Oracle, and SAP.

In this scenario, the resource isn't accessible after a system restart or a user logoff and logon.

Additionally, Windows can't access the SSL WebDav folder. Instead, it returns one of the following network error messages.

Error message 1

> Windows cannot access \\`server.company.com`@SSL\davWWWRoot\folder1\folder2\folder3\docs.
> Check the spelling of the name. Otherwise, there might be a problem with your network. To try to identify and resolve network problems, click diagnose.
> Error code: 0x80070035
> The network path was not found.

> ⓘ **Note**
>
> Error code 0x80070035 maps to ERROR_BAD_NETPATH.

Error message 2

> System Error 1244:
> The operation being requested was not performed because the user has not been authenticated.

> ⓘ **Note**
>
> Error code 1244 maps to ERROR_NOT_AUTHENTICATED.

Resolution

Starting in Windows 7, Basic Authentication cannot be persisted by the Credential Manager. The only method to reconnect in Basic Authentication mode is to disconnect and reconnect the drive. This is because WinHttp can't retrieve saved Basic Authentication or Digest Authentication credentials.

For persistent connections, make sure that an authentication scheme is selected that enables persistent credentials through a restart. For example, Kerberos enables persistent credentials for authentication or certificate-based authentication.

Workaround

Use a logon script that reconnects the DAV share at user logon. For example, include either of the following lines in the user logon script:

net use X: `http://server.company.com@8080/folder1/folder2/docs` /persistent:no

net use X: \\`server.company.com`@SSL\davWWWRoot\folder1\folder2\docs

> ⓘ **Note**
>
> 8080 is the TCP port number for the SSL connection to the DAV server.

Status

This behavior is by design in Basic Authentication mode in Windows 7.

More information

Basic Authentication is a widely used, industry-standard method for collecting user name and password information. The advantage of Basic Authentication is that it's part of the HTTP specification and is supported by most browsers.

However, Basic Authentication prompts the user for a user name and password. This information is then sent unencrypted over the network.

The Basic Authentication method isn't recommended unless you're sure that the connection between the user and the web server is secure (for example, by using SSL or a direct connection).

In Basic Authentication, the password is sent over the network in plain text. If this password is intercepted over the network by a network sniffer, an unauthorized user can determine the user name and password, and reuse these credentials.

It's because of this security risk that Office 2010 applications disable Basic Authentication over a non-SSL connection in the default configuration.

Specific situations

2123563 You cannot open Office file types directly from a server that supports only Basic authentication over a non-SSL connection

Basic authentication in Windows 7 isn't enabled by default if you're trying to connect to HTTP resources. For HTTP access, the BasicAuthLevel=2 key must be set (2 = Basic authentication enabled for SSL and for non-SSL connections).

If no proxy is configured, WinHTTP sends credentials only to local intranet sites. If an HTTP proxy program is running on the client, or if no proxy server entry is configured, and you try to connect to a resource by using an FQDN such as `http://server.company.com`, you should use the **AuthForwardServerList** registry key as described in KB 943280 to explicitly list the servers that you want to be treated as internal so that you can pass credentials for them.

943280 Prompt for Credentials When Accessing FQDN Sites From a Windows Vista or Windows 7 Computer

941050 Error message on a Windows Vista-based computer when you try to access a network drive that is mapped to a Web share: "The operation being requested was not performed because the user has not been authenticated"

References

WebDAV Redirector Registry Settings

Lost internet connectivity using VPN in Windows Defender Exploit Guard - Network Protection

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an error that occurs when you use the Network Protection feature in Windows Defender Exploit Guard in Audit or Block mode and a virtual private network (VPN).

Applies to: Windows 10 - all editions
Original KB number: 4560203

Symptoms

When using the Network Protection feature in Windows Defender Exploit Guard in Audit or Block mode and a virtual private network (VPN), you lose network connectivity and receive the **General Failure** error message when pinging an IP address.

Cause

This issue occurs because the current (4.12.x.x) antimalware platform update supporting the Network Protection feature is missing.

Solution

Install the latest (4.18.x.x) antimalware platform update as described here:

- Update for Windows Defender antimalware platform.
- Manage Windows Defender Antivirus updates and apply baselines.
- SCCM-Endpoint Protection: Enabling "Platform Update" for Microsoft Defender AV via SCCM ADR (Part 4).

Workaround

Set the following Group Policy to **Not Configured**:

Computer Configuration > Administrative Templates > Windows components > Windows Defender Antivirus > Windows Defender Exploit Guard > Network protection

> Prevent users and apps from accessing dangerous websites

Windows Firewall profile doesn't always switch to Domain when you use a third-party VPN client

Article • 09/23/2021 • 2 minutes to read

This article addresses an issue in which Windows Firewall profile doesn't switch from Public or Private to Domain when you connect to domain network by using a third-party VPN client.

Applies to: Windows 10 – all editions
Original KB number: 4550028

Symptoms

You use a third-party virtual private network (VPN) client to connect to a domain network. In this scenario, Windows Firewall doesn't always switch from the Public or Private profile to the Domain profile as expected.

Cause

A time lag in some third-party VPN clients sometimes causes this issue. The lag occurs when the client adds the necessary routes to the domain network.

Resolution

To fix this issue, we recommend that you contact the VPN provider for a solution to reduce the time lag caused by adding domain routes.

For VPN providers, you can use callback APIs to add routes as soon as the VPN adapter arrives at Windows. For example:

- **NotifyUnicastIpAddressChange**: Alerts callers of any changes to any IP address, including changes in DAD state.
- **NotifyIpInterfaceChange**: Registers a callback for notification of changes to all IP interfaces.

In user mode, there are IpHelper APIs. For example:

- **NotifyAddrChanget**: Notifies the user about address changes.

Workaround

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

To work around this issue, disable negative cache to help the Network Location Awareness (NLA) service when it retries domain detection. To do so, use the following methods.

- First, disable Domain Discovery negative cache by adding the **NegativeCachePeriod** registry key to following subkey:

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetLogon\Parameters`

  Name: **NegativeCachePeriod**
  Type: **REG_DWORD**
  Value Data: **0** (default value: **45** seconds; set to **0** to disable caching)

- If issue doesn't resolve, further disable DNS negative cache by adding the **MaxNegativeCacheTtl** registry key to the following subkey:

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters`

  Name: **MaxNegativeCacheTtl**
  Type: **REG_DWORD**
  Value Data: **0** (default value: **5** seconds; set to **0** to disable caching)

More information

When the issue occurs, the flow of events is as follows:

- The user connects to the VPN.
- During VPN tunnel setup, the VPN interface is created and assigned an IP address, and necessary routes are added to the interface. The following conditions apply:
  - TCP/IP immediately adds a host route and on-link subnet routes in one of the following situations:
    - The address is of a certain type, such as DHCP, IPv6 link local, and IPv6 temporary.

    - Optimistic Duplicate Address Detection (DAD) is enabled for that address.

      Otherwise, TCP/IP adds those routes after the DAD is successfully completed.

    - The VPN client is responsible for the necessary routes for the VPN networks, such as making the VPN interface routable to the VPN DNS server.
- The first route change triggers Network Connection Status Indicator (NCSI) detection. And the Network Location Awareness (NLA) service tries to authenticate to the domain controller to assign the correct profile to the firewall.
- The authentication starts by having the NLA service call the **DsGetDcName** function to retrieve the DC name. It's done by a DNS name resolution for the name, such as_ldap._tcp.CNNDC._sites.dc._msdcs.<domainname>.
- If this name resolution occurs before the necessary VPN routes to the VPN DNS server are added to the VPN interface, this DNS name resolution fails. And it returns "DsGetDcName function Failed with ERROR_NO_SUCH_DOMAIN." Then, this result is cached.
- The DNS name resolution failure might also create a negative DNS cache. The negative cache causes additional failure when the NLA service retries the domain detection.

Internet firewalls can prevent browsing and file sharing

Article • 04/06/2022 • 3 minutes to read

Turning on a firewall may prevent you from searching or sharing files with other computers on a home network.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 298804

Symptoms

After you enable an Internet firewall, you may not be able to search, or browse, for other computers on your home or office network. And you may not be able to share files with other computers on your home or office network. For example, when you enable the Internet Connection Firewall (ICF) feature in Windows XP, you find that you can't browse your network by using My Network Places. Also, if you use the `net view \\computername` command to view shares on a computer on your home or office network, you may receive the following error message:

> System error 6118 has occurred. The list of servers for this workgroup is not currently available.

Cause

This behavior may occur if you enable a firewall on the network connection that you use for your home or office network. By default, a firewall closes the ports that are used for file and print sharing. The purpose is to prevent Internet computers from connecting to file and print shares on your computer.

Resolution

To resolve this behavior, use a firewall only for network connections that you use to connect directly to the Internet. For example, use a firewall on a single computer that is connected to the Internet directly through a cable modem, a DSL modem, or a dial-up modem. If you use the same network connection to connect to both the Internet and a home or office network, use a router or firewall that prevents Internet computers from connecting to the shared resources on the home or office computers.

Don't use a firewall on network connections that you use to connect to your home or office network, unless the firewall can be configured to open ports only for your home or office network. If you connect to the Internet by using your home or office network, a firewall can be used only on the computer or the other device, such as a router, that provides the connection to the Internet. For example, if you connect to the Internet through a network that you manage, and that network uses connection sharing to provide Internet access to multiple computers, you can install or enable a firewall only on the shared Internet connection. If you connect to the Internet through a network that you do not manage, verify that your network administrator is using a firewall.

Status

This behavior is by design.

More information

A firewall is software or hardware that creates a protective barrier between your computer and potentially damaging content on the Internet. It helps guard your computer against malicious users and against many computer viruses and worms.

> **ⓘ Important**
>
> If you set up a firewall to help protect computer ports that are connected to the Internet, we do not recommend that you open these ports because they can be exposed to other computers on the Internet. Additionally, specific computers cannot be granted access to the open ports.

The following ports are associated with file sharing and server message block (SMB) communications:

- Microsoft file sharing SMB: User Datagram Protocol (UDP) ports from 135 through 139 and Transmission Control Protocol (TCP) ports from 135 through 139.
- Direct-hosted SMB traffic without a network basic input/output system (NetBIOS): port 445 (TCP and UDP).

Technical support for Windows x64 editions

Your hardware manufacturer provides technical support and assistance for Microsoft Windows x64 editions. Your hardware manufacturer provides support because a Windows x64 edition was included with your hardware. Your hardware manufacturer

might have customized the Windows x64 edition installation with unique components. Unique components might include specific device drivers or might include optional settings to maximize the performance of the hardware. Microsoft will provide reasonable-effort assistance if you need technical help with your Windows x64 edition. However, you might have to contact your manufacturer directly. Your manufacturer is best qualified to support the software that your manufacturer installed on the hardware.

For more information, see Protect my PC from viruses .

Advanced troubleshooting wireless network connectivity

Article • 09/02/2022 • 11 minutes to read

> **Note**
>
> Home users: This article is intended for use by support agents and IT professionals. If you're looking for more general information about Wi-Fi problems in Windows 10, check out this **Windows 10 Wi-Fi fix article**.

Applies to: Windows 10

Overview

This overview describes the general troubleshooting of establishing Wi-Fi connections from Windows clients. Troubleshooting Wi-Fi connections requires understanding the basic flow of the Wi-Fi autoconnect state machine. Understanding this flow makes it easier to determine the starting point in a repro scenario in which a different behavior is found.

This workflow involves knowledge and use of TextAnalysisTool, an extensive text filtering tool that is useful with complex traces with numerous ETW providers such as wireless_dbg trace scenario.

Scenarios

This article applies to any scenario in which Wi-Fi connections fail to establish. The troubleshooter is developed with Windows 10 clients in focus, but also may be useful with traces as far back as Windows 7.

> **Note**
>
> This troubleshooter uses examples that demonstrate a general strategy for navigating and interpreting wireless component **Event Tracing for Windows** (ETW). It's not meant to be representative of every wireless problem scenario.

Wireless ETW is incredibly verbose and calls out many innocuous errors (rather flagged behaviors that have little or nothing to do with the problem scenario). Searching for or

filtering on "err", "error", and "fail" will seldom lead you to the root cause of a problematic Wi-Fi scenario. Instead it will flood the screen with meaningless logs that will obfuscate the context of the actual problem.

It's important to understand the different Wi-Fi components involved, their expected behaviors, and how the problem scenario deviates from those expected behaviors. The intention of this troubleshooter is to show how to find a starting point in the verbosity of wireless_dbg ETW and home in on the responsible components that are causing the connection problem.

Known Issues and fixes

OS version	Fixed in
Windows 10, version 1803	KB4284848
Windows 10, version 1709	KB4284822
Windows 10, version 1703	KB4338827

Make sure that you install the latest Windows updates, cumulative updates, and rollup updates. To verify the update status, refer to the appropriate update-history webpage for your system:

- Windows 10 version 1809
- Windows 10 version 1803
- Windows 10 version 1709
- Windows 10 version 1703
- Windows 10 version 1607 and Windows Server 2016
- Windows 10 version 1511
- Windows 8.1 and Windows Server 2012 R2
- Windows Server 2012
- Windows 7 SP1 and Windows Server 2008 R2 SP1

Data Collection

1. Network Capture with ETW. Enter the following command at an elevated command prompt:

   Console

   ```
   netsh trace start wireless_dbg capture=yes overwrite=yes maxsize=4096
   tracefile=c:\tmp\wireless.etl
   ```

2. Reproduce the issue.

    - If there's a failure to establish connection, try to manually connect.
    - If it's intermittent but easily reproducible, try to manually connect until it fails. Record the time of each connection attempt, and whether it was a success or failure.
    - If the issue is intermittent but rare, netsh trace stop command needs to be triggered automatically (or at least alerted to admin quickly) to ensure trace doesn't overwrite the repro data.
    - If intermittent connection drops trigger stop command on a script (ping or test network constantly until fail, then netsh trace stop).

3. Stop the trace by entering the following command:

    ```
    Console

    netsh trace stop
    ```

4. To convert the output file to text format:

    ```
    Console

    netsh trace convert c:\tmp\wireless.etl
    ```

See the example ETW capture at the bottom of this article for an example of the command output. After running these commands, you'll have three files: wireless.cab, wireless.etl, and wireless.txt.

Troubleshooting

The following view is a high-level one of the main wifi components in Windows.

Wi-fi Components	Description
Windows Connection Manager (Wcmsvc)	The Windows Connection Manager (Wcmsvc) is closely associated with the UI controls (taskbar icon) to connect to various networks, including wireless networks. It accepts and processes input from the user and feeds it to the core wireless service.
WLAN Autoconfig Service (WlanSvc)	The WLAN Autoconfig Service (WlanSvc) handles the following core functions of wireless networks in windows: • Scanning for wireless networks in range • Managing connectivity of wireless networks

Wi-fi Components	Description
Media Specific Module (MSM)	The Media Specific Module (MSM) handles security aspects of connection being established.
Native Wifi stack	The Native WiFi stack consists of drivers and wireless APIs to interact with wireless miniports and the supporting user-mode Wlansvc.
Wifi miniport	Third-party wireless miniport drivers interface with the upper wireless stack to provide notifications to and receive commands from Windows.

The wifi connection state machine has the following states:

- Reset
- Ihv_Configuring
- Configuring
- Associating
- Authenticating
- Roaming
- Wait_For_Disconnected
- Disconnected

Standard wifi connections tend to transition between states such as:

- Connecting

  Reset --> Ihv_Configuring --> Configuring --> Associating --> Authenticating --> Connected

- Disconnecting

  Connected --> Roaming --> Wait_For_Disconnected --> Disconnected --> Reset

Filtering the ETW trace with the TextAnalysisTool (TAT) is an easy first step to determine where a failed connection setup is breaking down. A useful wifi filter file is included at the bottom of this article.

Use the **FSM transition** trace filter to see the connection state machine. You can see an example of this filter applied in the TAT at the bottom of this page.

An example of a good connection setup is:

```
Console
```

```
44676 [2]0F24.1020::2018-09-17 10:22:14.658 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Disconnected to State: Reset
45473 [1]0F24.1020::2018-09-17 10:22:14.667 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Reset to State: Ihv_Configuring
45597 [3]0F24.1020::2018-09-17 10:22:14.708 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Ihv_Configuring to State: Configuring
46085 [2]0F24.17E0::2018-09-17 10:22:14.710 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Configuring to State: Associating
47393 [1]0F24.1020::2018-09-17 10:22:14.879 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Associating to State: Authenticating
49465 [2]0F24.17E0::2018-09-17 10:22:14.990 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Authenticating to State: Connected
```

An example of a failed connection setup is:

Console

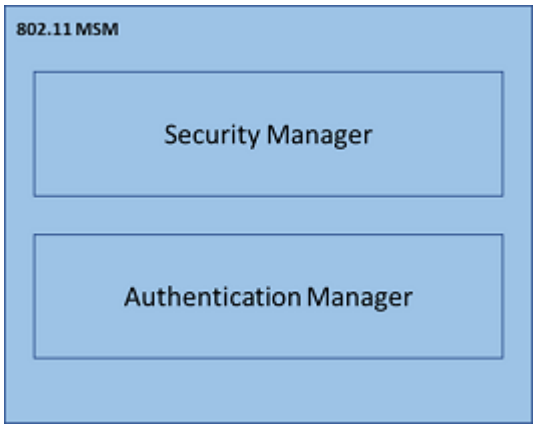
```
44676 [2]0F24.1020::2018-09-17 10:22:14.658 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Disconnected to State: Reset
45473 [1]0F24.1020::2018-09-17 10:22:14.667 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Reset to State: Ihv_Configuring
45597 [3]0F24.1020::2018-09-17 10:22:14.708 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Ihv_Configuring to State: Configuring
46085 [2]0F24.17E0::2018-09-17 10:22:14.710 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Configuring to State: Associating
47393 [1]0F24.1020::2018-09-17 10:22:14.879 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Associating to State: Authenticating
49465 [2]0F24.17E0::2018-09-17 10:22:14.990 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State: Authenticating to State: Roaming
```

By identifying the state at which the connection fails, one can focus more specifically in the trace on logs prior to the last known good state

Examining [Microsoft-Windows-WLAN-AutoConfig] logs prior to the bad state change should show evidence of error. Often, however, the error is propagated up through other wireless components. In many cases the next component of interest will be the MSM, which lies just below Wlansvc.

The important components of the MSM include:

- Security Manager (SecMgr) - handles all pre and post-connection security operations.
- Authentication Engine (AuthMgr) – Manages 802.1x auth requests



Each of these components has its own individual state machines that follow specific transitions. Enable the `FSM transition`, `SecMgr Transition`, and `AuthMgr Transition` filters in TextAnalysisTool for more detail.

Further to the preceding example, the combined filters look like the following command example:

Console

```
[2] 0C34.2FF0::08/28/17-13:24:28.693 [Microsoft-Windows-WLAN-AutoConfig]FSM
Transition from State:
Reset to State: Ihv_Configuring
[2] 0C34.2FF0::08/28/17-13:24:28.693 [Microsoft-Windows-WLAN-AutoConfig]FSM
Transition from State:
Ihv_Configuring to State: Configuring
[1] 0C34.2FE8::08/28/17-13:24:28.711 [Microsoft-Windows-WLAN-AutoConfig]FSM
Transition from State:
Configuring to State: Associating
[0] 0C34.275C::08/28/17-13:24:28.902 [Microsoft-Windows-WLAN-
AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition INACTIVE (1) --
> ACTIVE (2)
[0] 0C34.275C::08/28/17-13:24:28.902 [Microsoft-Windows-WLAN-
AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition ACTIVE (2) -->
START AUTH (3)
[4] 0EF8.0708::08/28/17-13:24:28.928 [Microsoft-Windows-WLAN-AutoConfig]Port
(14) Peer 0x186472F64FD2 AuthMgr Transition ENABLED  --> START_AUTH
[3] 0C34.2FE8::08/28/17-13:24:28.902 [Microsoft-Windows-WLAN-AutoConfig]FSM
Transition from State:
Associating to State: Authenticating
[1] 0C34.275C::08/28/17-13:24:28.960 [Microsoft-Windows-WLAN-
AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition START AUTH (3)
--> WAIT FOR AUTH SUCCESS (4)
[4] 0EF8.0708::08/28/17-13:24:28.962 [Microsoft-Windows-WLAN-AutoConfig]Port
(14) Peer 0x186472F64FD2 AuthMgr Transition START_AUTH  --> AUTHENTICATING
[2] 0C34.2FF0::08/28/17-13:24:29.751 [Microsoft-Windows-WLAN-
AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition WAIT FOR AUTH
SUCCESS (7) --> DEACTIVATE (11)
[2] 0C34.2FF0::08/28/17-13:24:29.7512788 [Microsoft-Windows-WLAN-
AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition DEACTIVATE (11)
--> INACTIVE (1)
```

```
[2] 0C34.2FF0::08/28/17-13:24:29.7513404 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State:
Authenticating to State: Roaming
```

> **Note**
>
> In the next to last line the SecMgr transition is suddenly deactivating:
> [2] 0C34.2FF0::08/28/17-13:24:29.7512788 [Microsoft-Windows-WLAN-AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition DEACTIVATE (11) --> INACTIVE (1)
>
> This transition is what eventually propagates to the main connection state machine and causes the Authenticating phase to devolve to Roaming state. As before, it makes sense to focus on tracing prior to this SecMgr behavior to determine the reason for the deactivation.

Enabling the `Microsoft-Windows-WLAN-AutoConfig` filter will show more detail leading to the DEACTIVATE transition:

Console

```
[3] 0C34.2FE8::08/28/17-13:24:28.902 [Microsoft-Windows-WLAN-AutoConfig]FSM
Transition from State:
Associating to State: Authenticating
[1] 0C34.275C::08/28/17-13:24:28.960 [Microsoft-Windows-WLAN-
AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition START AUTH (3)
--> WAIT FOR AUTH SUCCESS (4)
[4] 0EF8.0708::08/28/17-13:24:28.962 [Microsoft-Windows-WLAN-AutoConfig]Port
(14) Peer 0x186472F64FD2 AuthMgr Transition START_AUTH  --> AUTHENTICATING
[0]0EF8.2EF4::08/28/17-13:24:29.549 [Microsoft-Windows-WLAN-
AutoConfig]Received Security Packet: PHY_STATE_CHANGE
[0]0EF8.2EF4::08/28/17-13:24:29.549 [Microsoft-Windows-WLAN-
AutoConfig]Change radio state for interface = Intel(R) Centrino(R) Ultimate-
N 6300 AGN :  PHY = 3, software state = on , hardware state = off )
[0] 0EF8.1174::08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-
AutoConfig]Received Security Packet: PORT_DOWN
[0] 0EF8.1174::08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-AutoConfig]FSM
Current state Authenticating , event Upcall_Port_Down
[0] 0EF8.1174:: 08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-
AutoConfig]Received IHV PORT DOWN, peer 0x186472F64FD2
[2] 0C34.2FF0::08/28/17-13:24:29.751 [Microsoft-Windows-WLAN-
AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition WAIT FOR AUTH
SUCCESS (7) --> DEACTIVATE (11)
 [2] 0C34.2FF0::08/28/17-13:24:29.7512788 [Microsoft-Windows-WLAN-
AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition DEACTIVATE (11)
--> INACTIVE (1)
[2] 0C34.2FF0::08/28/17-13:24:29.7513404 [Microsoft-Windows-WLAN-
```

```
AutoConfig]FSM Transition from State:
Authenticating to State: Roaming
```

The trail backwards reveals a Port Down notification:

[0] 0EF8.1174:: 08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-AutoConfig]Received IHV PORT DOWN, peer 0x186472F64FD2

Port events indicate changes closer to the wireless hardware. The trail can be followed by continuing to see the origin of this indication.

Below, the MSM is the native wifi stack. These drivers are Windows native wifi drivers that talk to the wifi miniport drivers. It's responsible for converting Wi-Fi (802.11) packets to 802.3 (Ethernet) so that TCPIP and other protocols and can use it.

Enable trace filter for `[Microsoft-Windows-NWifi]`:

Console

```
[3] 0C34.2FE8::08/28/17-13:24:28.902 [Microsoft-Windows-WLAN-AutoConfig]FSM
Transition from State:
Associating to State: Authenticating
[1] 0C34.275C::08/28/17-13:24:28.960 [Microsoft-Windows-WLAN-
AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition START AUTH (3)
--> WAIT FOR AUTH SUCCESS (4)
[4] 0EF8.0708::08/28/17-13:24:28.962 [Microsoft-Windows-WLAN-AutoConfig]Port
(14) Peer 0x8A1514B62510 AuthMgr Transition START_AUTH  --> AUTHENTICATING
[0]0000.0000::08/28/17-13:24:29.127 [Microsoft-Windows-NWiFi]DisAssoc:
0x8A1514B62510 Reason: 0x4
[0]0EF8.2EF4::08/28/17-13:24:29.549 [Microsoft-Windows-WLAN-
AutoConfig]Received Security Packet: PHY_STATE_CHANGE
[0]0EF8.2EF4::08/28/17-13:24:29.549 [Microsoft-Windows-WLAN-
AutoConfig]Change radio state for interface = Intel(R) Centrino(R) Ultimate-
N 6300 AGN :  PHY = 3, software state = on , hardware state = off )
[0] 0EF8.1174::08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-
AutoConfig]Received Security Packet: PORT_DOWN
[0] 0EF8.1174::08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-AutoConfig]FSM
Current state Authenticating , event Upcall_Port_Down
[0] 0EF8.1174:: 08/28/17-13:24:29.705 [Microsoft-Windows-WLAN-
AutoConfig]Received IHV PORT DOWN, peer 0x186472F64FD2
[2] 0C34.2FF0::08/28/17-13:24:29.751 [Microsoft-Windows-WLAN-
AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition WAIT FOR AUTH
SUCCESS (7) --> DEACTIVATE (11)
 [2] 0C34.2FF0::08/28/17-13:24:29.7512788 [Microsoft-Windows-WLAN-
AutoConfig]Port[13] Peer 8A:15:14:B6:25:10 SecMgr Transition DEACTIVATE (11)
--> INACTIVE (1)
[2] 0C34.2FF0::08/28/17-13:24:29.7513404 [Microsoft-Windows-WLAN-
AutoConfig]FSM Transition from State:
Authenticating to State: Roaming
```

In the trace above, we see the line:

Console

```
[0]0000.0000::08/28/17-13:24:29.127 [Microsoft-Windows-NWiFi]DisAssoc:
0x8A1514B62510 Reason: 0x4
```

This line is followed by PHY_STATE_CHANGE and PORT_DOWN events due to a disassociate coming from the Access Point (AP), as an indication to deny the connection. This denail could be due to invalid credentials, connection parameters, loss of signal/roaming, and various other reasons for aborting a connection. The action here would be to examine the reason for the disassociate sent from the indicated AP MAC (8A:15:14:B6:25:10). This action would be done by examining internal logging/tracing from the AP.

More information

- 802.11 Wireless Tools and Settings
- Understanding 802.1X authentication for wireless networks

Example ETW capture

Console

```
C:\tmp>netsh trace start wireless_dbg capture=yes overwrite=yes maxsize=4096
tracefile=c:\tmp\wireless.etl

Trace configuration:
-----------------------------------------------------------------
Status:             Running
Trace File:         C:\tmp\wireless.etl
Append:             Off
Circular:           On
Max Size:           4096 MB
Report:             Off

C:\tmp>netsh trace stop
Correlating traces ... done
Merging traces ... done
Generating data collection ... done
The trace file and additional troubleshooting information have been compiled
as "c:\tmp\wireless.cab".
File location = c:\tmp\wireless.etl
Tracing session was successfully stopped.

C:\tmp>netsh trace convert c:\tmp\wireless.etl
```

```
Input file:  c:\tmp\wireless.etl
Dump file:   c:\tmp\wireless.txt
Dump format: TXT
Report file: -
Generating dump ... done

C:\tmp>dir
 Volume in drive C has no label.
 Volume Serial Number is 58A8-7DE5

 Directory of C:\tmp

01/09/2019  02:59 PM    [DIR]          .
01/09/2019  02:59 PM    [DIR]          ..
01/09/2019  02:59 PM         4,855,952 wireless.cab
01/09/2019  02:56 PM         2,752,512 wireless.etl
01/09/2019  02:59 PM         2,786,540 wireless.txt
               3 File(s)     10,395,004 bytes
               2 Dir(s)  46,648,332,288 bytes free
```

Wifi filter file

Copy and paste all the lines below and save them into a text file named *wifi.tat*. Load the filter file into the TextAnalysisTool by selecting **File** > **Load Filters**.

XML

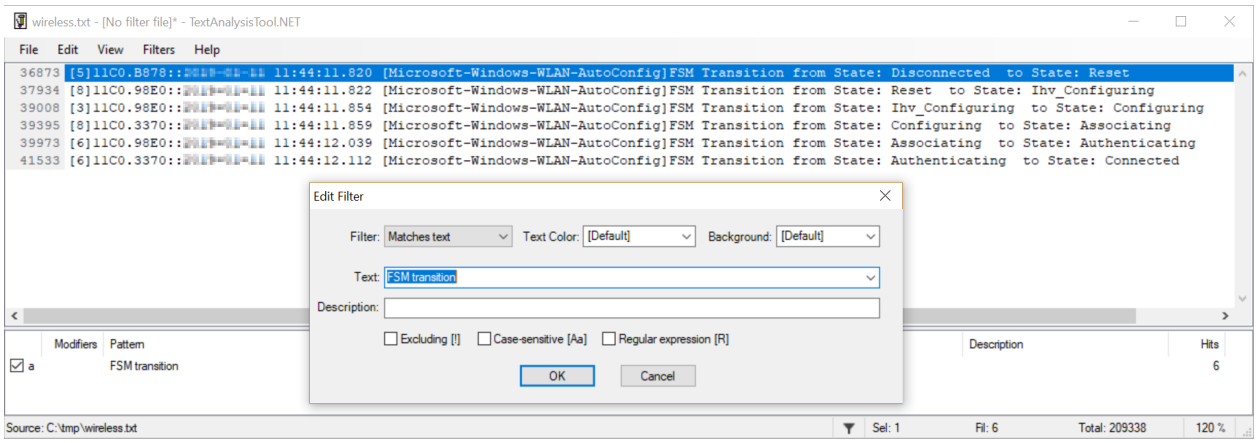
```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<TextAnalysisTool.NET version="2018-01-03" showOnlyFilteredLines="False">
  <filters>
    <filter enabled="n" excluding="n" description="" foreColor="000000"
backColor="d3d3d3" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-OneX]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Unknown]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-EapHost]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[]***" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-Winsock-AFD]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-WinHttp]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-WebIO]" />
```

```
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-Winsock-NameResolution]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-TCPIP]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-DNS-Client]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-NlaSvc]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-Iphlpsvc-Trace]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-DHCPv6-Client]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-Dhcp-Client]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-NCSI]" />
    <filter enabled="y" excluding="n" description="" backColor="90ee90"
type="matches_text" case_sensitive="n" regex="n" text="AuthMgr Transition"
/>
    <filter enabled="y" excluding="n" description="" foreColor="0000ff"
backColor="add8e6" type="matches_text" case_sensitive="n" regex="n"
text="FSM transition" />
    <filter enabled="y" excluding="n" description="" foreColor="000000"
backColor="dda0dd" type="matches_text" case_sensitive="n" regex="n"
text="SecMgr transition" />
    <filter enabled="y" excluding="n" description="" foreColor="000000"
backColor="f08080" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-NWiFi]" />
    <filter enabled="y" excluding="n" description="" foreColor="000000"
backColor="ffb6c1" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-WiFiNetworkManager]" />
    <filter enabled="y" excluding="n" description="" foreColor="000000"
backColor="dda0dd" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-WLAN-AutoConfig]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-NetworkProfile]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-WFP]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[Microsoft-Windows-WinINet]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n" text="
[MSNT_SystemTrace]" />
    <filter enabled="y" excluding="y" description="" foreColor="000000"
```

```
backColor="ffffff" type="matches_text" case_sensitive="n" regex="n"
text="Security]Capability" />
  </filters>
</TextAnalysisTool.NET>
```

TextAnalysisTool example

In the following example, the **View** settings are configured to **Show Only Filtered Lines**.



Data collection for troubleshooting 802.1X authentication

Article • 09/02/2022 • 8 minutes to read

Use the following steps to collect data that can be used to troubleshoot 802.1X authentication issues. When you have collected data, see Advanced troubleshooting 802.1X authentication.

Applies to: Windows 10

Capture wireless/wired functionality logs

Use the following steps to collect wireless and wired logs on Windows and Windows Server:

1. Create *C:\MSLOG* on the client machine to store captured logs.
2. Launch an elevated command prompt on the client machine, and run the following commands to start a RAS trace log and a Wireless/Wired scenario log.

   Wireless Windows 8.1, Windows 10, and Windows 11:

   Console

   ```
   netsh ras set tracing * enabled
   netsh trace start scenario=wlan,wlan_wpp,wlan_dbg,wireless_dbg
   globallevel=0xff capture=yes maxsize=1024
   tracefile=C:\MSLOG\%COMPUTERNAME%_wireless_cli.etl
   ```

   Wireless Windows 7 and Windows 8:

   Console

   ```
   netsh ras set tracing * enabled
   netsh trace start scenario=wlan,wlan_wpp,wlan_dbg globallevel=0xff
   capture=yes maxsize=1024
   tracefile=C:\MSLOG\%COMPUTERNAME%_wireless_cli.etl
   ```

   Wired client, regardless of version

   Console

```
netsh ras set tracing * enabled
netsh trace start scenario=lan globallevel=0xff capture=yes
maxsize=1024 tracefile=C:\MSLOG\%COMPUTERNAME%_wired_cli.etl
```

3. Run the following command to enable CAPI2 logging and increase the size:

```
Console

wevtutil.exe sl Microsoft-Windows-CAPI2/Operational /e:true
wevtutil sl Microsoft-Windows-CAPI2/Operational /ms:104857600
```

4. Create *C:\MSLOG* on the NPS to store captured logs.

5. Launch an elevated command prompt on the NPS server and run the following commands to start a RAS trace log and a Wireless/Wired scenario log:

   Windows Server 2012 R2, Windows Server 2016 wireless network:

```
Console

netsh ras set tracing * enabled
netsh trace start scenario=wlan,wlan_wpp,wlan_dbg,wireless_dbg
globallevel=0xff capture=yes maxsize=1024
tracefile=C:\MSLOG\%COMPUTERNAME%_wireless_nps.etl
```

   Windows Server 2008 R2, Windows Server 2012 wireless network

```
Console

netsh ras set tracing * enabled
netsh trace start scenario=wlan,wlan_wpp,wlan_dbg globallevel=0xff
capture=yes maxsize=1024
tracefile=C:\MSLOG\%COMPUTERNAME%_wireless_nps.etl
```

   Wired network

```
Console

netsh ras set tracing * enabled
netsh trace start scenario=lan globallevel=0xff capture=yes
maxsize=1024 tracefile=C:\MSLOG\%COMPUTERNAME%_wired_nps.etl
```

6. Run the following command to enable CAPI2 logging and increase the size:

```
Console
```

```
wevtutil.exe sl Microsoft-Windows-CAPI2/Operational /e:true
wevtutil sl Microsoft-Windows-CAPI2/Operational /ms:104857600
```

7. Run the following command from the command prompt on the client machine and start PSR to capture screen images:

> **Note**
>
> When the mouse button is clicked, the cursor will blink in red while capturing a screen image.

Console

```
psr /start /output c:\MSLOG\%computername%_psr.zip /maxsc 100
```

8. Repro the issue.

9. Run the following command on the client PC to stop the PSR capturing:

Console

```
psr /stop
```

10. Run the following commands from the command prompt on the NPS server.

    - To stop RAS trace log and wireless scenario log:

      Console

      ```
      netsh trace stop
      netsh ras set tracing * disabled
      ```

    - To disable and copy CAPI2 log:

      Console

      ```
      wevtutil.exe sl Microsoft-Windows-CAPI2/Operational /e:false
      wevtutil.exe epl Microsoft-Windows-CAPI2/Operational
      C:\MSLOG\%COMPUTERNAME%_CAPI2.evtx
      ```

11. Run the following commands on the client PC.

    - To stop RAS trace log and wireless scenario log:

```
Console

netsh trace stop
netsh ras set tracing * disabled
```

- To disable and copy the CAPI2 log:

```
Console

wevtutil.exe sl Microsoft-Windows-CAPI2/Operational /e:false
wevtutil.exe epl Microsoft-Windows-CAPI2/Operational
C:\MSLOG\%COMPUTERNAME%_CAPI2.evtx
```

12. Save the following logs on the client and the NPS:

    Client

    - *C:\MSLOG\%computername%_psr.zip*
    - *C:\MSLOG\%COMPUTERNAME%_CAPI2.evtx*
    - *C:\MSLOG\%COMPUTERNAME%_wireless_cli.etl*
    - *C:\MSLOG\%COMPUTERNAME%_wireless_cli.cab*
    - All log files and folders in *%Systemroot%\Tracing*

    NPS

    - *C\MSLOG\%COMPUTERNAME%_CAPI2.evtx*
    - *C:\MSLOG\%COMPUTERNAME%_wireless_nps.etl* (*%COMPUTERNAME%_wired_nps.etl* for wired scenario)
    - *C:\MSLOG\%COMPUTERNAME%_wireless_nps.cab* (*%COMPUTERNAME%_wired_nps.cab* for wired scenario)
    - All log files and folders in *%Systemroot%\Tracing*

Save environment and configuration information

On Windows client

1. Create *C:\MSLOG* to store captured logs.
2. Launch a command prompt as an administrator.
3. Run the following commands.

- Environment information and Group Policy application status

```
Console

gpresult /H C:\MSLOG\%COMPUTERNAME%_gpresult.htm
msinfo32 /report c:\MSLOG\%COMPUTERNAME%_msinfo32.txt
ipconfig /all > c:\MSLOG\%COMPUTERNAME%_ipconfig.txt
route print > c:\MSLOG\%COMPUTERNAME%_route_print.txt
```

- Event logs

```
Console

wevtutil epl Application c:\MSLOG\%COMPUTERNAME%_Application.evtx
wevtutil epl System c:\MSLOG\%COMPUTERNAME%_System.evtx
wevtutil epl Security c:\MSLOG\%COMPUTERNAME%_Security.evtx
wevtutil epl Microsoft-Windows-GroupPolicy/Operational
C:\MSLOG\%COMPUTERNAME%_GroupPolicy_Operational.evtx
wevtutil epl "Microsoft-Windows-WLAN-AutoConfig/Operational"
c:\MSLOG\%COMPUTERNAME%_Microsoft-Windows-WLAN-AutoConfig-
Operational.evtx
wevtutil epl "Microsoft-Windows-Wired-AutoConfig/Operational"
c:\MSLOG\%COMPUTERNAME%_Microsoft-Windows-Wired-AutoConfig-
Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-
CredentialRoaming/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-
CredentialRoaming_Operational.evtx
wevtutil epl Microsoft-Windows-CertPoleEng/Operational
c:\MSLOG\%COMPUTERNAME%_CertPoleEng_Operational.evtx
```

- For Windows 8 and later, also run these commands for event logs:

```
Console

wevtutil epl Microsoft-Windows-CertificateServicesClient-
Lifecycle-System/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-
System_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-
Lifecycle-User/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-
User_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServices-
Deployment/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServices-
Deployment_Operational.evtx
```

- Certificates Store information:

Console

```
certutil -v -silent -store MY > c:\MSLOG\%COMPUTERNAME%_cert-
Personal-Registry.txt
certutil -v -silent -store ROOT > c:\MSLOG\%COMPUTERNAME%_cert-
TrustedRootCA-Registry.txt
certutil -v -silent -store -grouppolicy ROOT >
c:\MSLOG\%COMPUTERNAME%_cert-TrustedRootCA-GroupPolicy.txt
certutil -v -silent -store -enterprise ROOT >
c:\MSLOG\%COMPUTERNAME%_TrustedRootCA-Enterprise.txt
certutil -v -silent -store TRUST > c:\MSLOG\%COMPUTERNAME%_cert-
EnterpriseTrust-Reg.txt
certutil -v -silent -store -grouppolicy TRUST >
c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-GroupPolicy.txt
certutil -v -silent -store -enterprise TRUST >
c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-Enterprise.txt
certutil -v -silent -store CA > c:\MSLOG\%COMPUTERNAME%_cert-
IntermediateCA-Registry.txt
certutil -v -silent -store -grouppolicy CA >
c:\MSLOG\%COMPUTERNAME%_cert-IntermediateCA-GroupPolicy.txt
certutil -v -silent -store -enterprise CA >
c:\MSLOG\%COMPUTERNAME%_cert-Intermediate-Enterprise.txt
certutil -v -silent -store AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-Registry.txt
certutil -v -silent -store -grouppolicy AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-GroupPolicy.txt
certutil -v -silent -store -enterprise AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-Enterprise.txt
certutil -v -silent -store SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-Registry.txt
certutil -v -silent -store -grouppolicy SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-GroupPolicy.txt
certutil -v -silent -store -enterprise SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-Enterprise.txt
certutil -v -silent -store -enterprise NTAUTH >
c:\MSLOG\%COMPUTERNAME%_cert-NtAuth-Enterprise.txt
certutil -v -silent -user -store MY >
c:\MSLOG\%COMPUTERNAME%_cert-User-Personal-Registry.txt
certutil -v -silent -user -store ROOT >
c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-Registry.txt
certutil -v -silent -user -store -enterprise ROOT >
c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-Enterprise.txt
certutil -v -silent -user -store TRUST >
c:\MSLOG\%COMPUTERNAME%_cert-User-EnterpriseTrust-Registry.txt
certutil -v -silent -user -store -grouppolicy TRUST >
c:\MSLOG\%COMPUTERNAME%_cert-User-EnterpriseTrust-GroupPolicy.txt
certutil -v -silent -user -store CA >
c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-Registry.txt
certutil -v -silent -user -store -grouppolicy CA >
c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-GroupPolicy.txt
certutil -v -silent -user -store Disallowed >
c:\MSLOG\%COMPUTERNAME%_cert-User-UntrustedCertificates-
Registry.txt
certutil -v -silent -user -store -grouppolicy Disallowed >
```

```
c:\MSLOG\%COMPUTERNAME%_cert-User-UntrustedCertificates-
GroupPolicy.txt
certutil -v -silent -user -store AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-3rdPartyRootCA-Registry.txt
certutil -v -silent -user -store -grouppolicy AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-3rdPartyRootCA-GroupPolicy.txt
certutil -v -silent -user -store SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-SmartCardRoot-Registry.txt
certutil -v -silent -user -store -grouppolicy SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-SmartCardRoot-GroupPolicy.txt
certutil -v -silent -user -store UserDS >
c:\MSLOG\%COMPUTERNAME%_cert-User-UserDS.txt
```

- Wireless LAN client information:

```
Console

netsh wlan show all > c:\MSLOG\%COMPUTERNAME%_wlan_show_all.txt
netsh wlan export profile folder=c:\MSLOG\
```

- Wired LAN Client information

```
Console

netsh lan show interfaces >
c:\MSLOG\%computername%_lan_interfaces.txt
netsh lan show profiles > c:\MSLOG\%computername%_lan_profiles.txt
netsh lan show settings > c:\MSLOG\%computername%_lan_settings.txt
netsh lan export profile folder=c:\MSLOG\
```

4. Save the logs stored in *C:\MSLOG*.

On NPS

1. Create *C:\MSLOG* to store captured logs.

2. Launch a command prompt as an administrator.

3. Run the following commands.

- Environmental information and Group Policies application status:

```
Console

gpresult /H C:\MSLOG\%COMPUTERNAME%_gpresult.txt
msinfo32 /report c:\MSLOG\%COMPUTERNAME%_msinfo32.txt
ipconfig /all > c:\MSLOG\%COMPUTERNAME%_ipconfig.txt
route print > c:\MSLOG\%COMPUTERNAME%_route_print.txt
```

- Event logs:

```
Console

wevtutil epl Application c:\MSLOG\%COMPUTERNAME%_Application.evtx
wevtutil epl System c:\MSLOG\%COMPUTERNAME%_System.evtx
wevtutil epl Security c:\MSLOG\%COMPUTERNAME%_Security.evtx
wevtutil epl Microsoft-Windows-GroupPolicy/Operational
c:\MSLOG\%COMPUTERNAME%_GroupPolicy_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-
CredentialRoaming/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-
CredentialRoaming_Operational.evtx
wevtutil epl Microsoft-Windows-CertPoleEng/Operational
c:\MSLOG\%COMPUTERNAME%_CertPoleEng_Operational.evtx
```

- Run the following commands on Windows Server 2012 and later:

```
Console

wevtutil epl Microsoft-Windows-CertificateServicesClient-
Lifecycle-System/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-
System_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-
Lifecycle-User/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-
User_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServices-
Deployment/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServices-
Deployment_Operational.evtx
```

- Certificates store information

```
Console

certutil -v -silent -store MY > c:\MSLOG\%COMPUTERNAME%_cert-
Personal-Registry.txt
certutil -v -silent -store ROOT > c:\MSLOG\%COMPUTERNAME%_cert-
TrustedRootCA-Registry.txt
certutil -v -silent -store -grouppolicy ROOT >
c:\MSLOG\%COMPUTERNAME%_cert-TrustedRootCA-GroupPolicy.txt
certutil -v -silent -store -enterprise ROOT >
c:\MSLOG\%COMPUTERNAME%_TrustedRootCA-Enterprise.txt
certutil -v -silent -store TRUST > c:\MSLOG\%COMPUTERNAME%_cert-
EnterpriseTrust-Reg.txt
certutil -v -silent -store -grouppolicy TRUST >
c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-GroupPolicy.txt
certutil -v -silent -store -enterprise TRUST >
```

```
c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-Enterprise.txt
certutil -v -silent -store CA > c:\MSLOG\%COMPUTERNAME%_cert-
IntermediateCA-Registry.txt
certutil -v -silent -store -grouppolicy CA >
c:\MSLOG\%COMPUTERNAME%_cert-IntermediateCA-GroupPolicy.txt
certutil -v -silent -store -enterprise CA >
c:\MSLOG\%COMPUTERNAME%_cert-Intermediate-Enterprise.txt
certutil -v -silent -store AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-Registry.txt
certutil -v -silent -store -grouppolicy AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-GroupPolicy.txt
certutil -v -silent -store -enterprise AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-Enterprise.txt
certutil -v -silent -store SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-Registry.txt
certutil -v -silent -store -grouppolicy SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-GroupPolicy.txt
certutil -v -silent -store -enterprise SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-Enterprise.txt
certutil -v -silent -store -enterprise NTAUTH >
c:\MSLOG\%COMPUTERNAME%_cert-NtAuth-Enterprise.txt
certutil -v -silent -user -store MY >
c:\MSLOG\%COMPUTERNAME%_cert-User-Personal-Registry.txt
certutil -v -silent -user -store ROOT >
c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-Registry.txt
certutil -v -silent -user -store -enterprise ROOT >
c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-Enterprise.txt
certutil -v -silent -user -store TRUST >
c:\MSLOG\%COMPUTERNAME%_cert-User-EnterpriseTrust-Registry.txt
certutil -v -silent -user -store -grouppolicy TRUST >
c:\MSLOG\%COMPUTERNAME%_cert-User-EnterpriseTrust-GroupPolicy.txt
certutil -v -silent -user -store CA >
c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-Registry.txt
certutil -v -silent -user -store -grouppolicy CA >
c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-GroupPolicy.txt
certutil -v -silent -user -store Disallowed >
c:\MSLOG\%COMPUTERNAME%_cert-User-UntrustedCertificates-
Registry.txt
certutil -v -silent -user -store -grouppolicy Disallowed >
c:\MSLOG\%COMPUTERNAME%_cert-User-UntrustedCertificates-
GroupPolicy.txt
certutil -v -silent -user -store AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-3rdPartyRootCA-Registry.txt
certutil -v -silent -user -store -grouppolicy AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-3rdPartyRootCA-GroupPolicy.txt
certutil -v -silent -user -store SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-SmartCardRoot-Registry.txt
certutil -v -silent -user -store -grouppolicy SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-SmartCardRoot-GroupPolicy.txt
certutil -v -silent -user -store UserDS >
c:\MSLOG\%COMPUTERNAME%_cert-User-UserDS.txt
```

- NPS configuration information:

```
Console

netsh nps show config >
C:\MSLOG\%COMPUTERNAME%_nps_show_config.txt
netsh nps export filename=C:\MSLOG\%COMPUTERNAME%_nps_export.xml
exportPSK=YES
```

4. Take the following steps to save an NPS accounting log.
   a. Open **Administrative tools** > **Network Policy Server**.
   b. On the Network Policy Server administration tool, select **Accounting** in the left pane.
   c. Select **Change Log File Properties**.
   d. On the **Log File** tab, note the log file naming convention shown as **Name** and the log file location shown in **Directory** box.
   e. Copy the log file to *C:\MSLOG*.

5. Save the logs stored in *C:\MSLOG*.

Certification Authority (CA) (OPTIONAL)

1. On a CA, launch a command prompt as an administrator. Create *C:\MSLOG* to store captured logs.

2. Run the following commands.

   - Environmental information and Group Policies application status

```
Console

gpresult /H C:\MSLOG\%COMPUTERNAME%_gpresult.txt
msinfo32 /report c:\MSLOG\%COMPUTERNAME%_msinfo32.txt
ipconfig /all > c:\MSLOG\%COMPUTERNAME%_ipconfig.txt
route print > c:\MSLOG\%COMPUTERNAME%_route_print.txt
```

   - Event logs

```
Console

wevtutil epl Application c:\MSLOG\%COMPUTERNAME%_Application.evtx
wevtutil epl System c:\MSLOG\%COMPUTERNAME%_System.evtx
wevtutil epl Security c:\MSLOG\%COMPUTERNAME%_Security.evtx
wevtutil epl Microsoft-Windows-GroupPolicy/Operational
c:\MSLOG\%COMPUTERNAME%_GroupPolicy_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-
CredentialRoaming/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-
```

```
CredentialRoaming_Operational.evtx
wevtutil epl Microsoft-Windows-CertPoleEng/Operational
c:\MSLOG\%COMPUTERNAME%_CertPoleEng_Operational.evtx
```

- Run the following lines on Windows 2012 and up

Console

```
wevtutil epl Microsoft-Windows-CertificateServicesClient-
Lifecycle-System/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-
System_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServicesClient-
Lifecycle-User/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServicesClient-Lifecycle-
User_Operational.evtx
wevtutil epl Microsoft-Windows-CertificateServices-
Deployment/Operational
c:\MSLOG\%COMPUTERNAME%_CertificateServices-
Deployment_Operational.evtx
```

- Certificates store information

Console

```
certutil -v -silent -store MY > c:\MSLOG\%COMPUTERNAME%_cert-
Personal-Registry.txt
certutil -v -silent -store ROOT > c:\MSLOG\%COMPUTERNAME%_cert-
TrustedRootCA-Registry.txt
certutil -v -silent -store -grouppolicy ROOT >
c:\MSLOG\%COMPUTERNAME%_cert-TrustedRootCA-GroupPolicy.txt
certutil -v -silent -store -enterprise ROOT >
c:\MSLOG\%COMPUTERNAME%_TrustedRootCA-Enterprise.txt
certutil -v -silent -store TRUST > c:\MSLOG\%COMPUTERNAME%_cert-
EnterpriseTrust-Reg.txt
certutil -v -silent -store -grouppolicy TRUST >
c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-GroupPolicy.txt
certutil -v -silent -store -enterprise TRUST >
c:\MSLOG\%COMPUTERNAME%_cert-EnterpriseTrust-Enterprise.txt
certutil -v -silent -store CA > c:\MSLOG\%COMPUTERNAME%_cert-
IntermediateCA-Registry.txt
certutil -v -silent -store -grouppolicy CA >
c:\MSLOG\%COMPUTERNAME%_cert-IntermediateCA-GroupPolicy.txt
certutil -v -silent -store -enterprise CA >
c:\MSLOG\%COMPUTERNAME%_cert-Intermediate-Enterprise.txt
certutil -v -silent -store AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-Registry.txt
certutil -v -silent -store -grouppolicy AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-GroupPolicy.txt
certutil -v -silent -store -enterprise AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-3rdPartyRootCA-Enterprise.txt
certutil -v -silent -store SmartCardRoot >
```

```
c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-Registry.txt
certutil -v -silent -store -grouppolicy SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-GroupPolicy.txt
certutil -v -silent -store -enterprise SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-SmartCardRoot-Enterprise.txt
certutil -v -silent -store -enterprise NTAUTH >
c:\MSLOG\%COMPUTERNAME%_cert-NtAuth-Enterprise.txt
certutil -v -silent -user -store MY >
c:\MSLOG\%COMPUTERNAME%_cert-User-Personal-Registry.txt
certutil -v -silent -user -store ROOT >
c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-Registry.txt
certutil -v -silent -user -store -enterprise ROOT >
c:\MSLOG\%COMPUTERNAME%_cert-User-TrustedRootCA-Enterprise.txt
certutil -v -silent -user -store TRUST >
c:\MSLOG\%COMPUTERNAME%_cert-User-EnterpriseTrust-Registry.txt
certutil -v -silent -user -store -grouppolicy TRUST >
c:\MSLOG\%COMPUTERNAME%_cert-User-EnterpriseTrust-GroupPolicy.txt
certutil -v -silent -user -store CA >
c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-Registry.txt
certutil -v -silent -user -store -grouppolicy CA >
c:\MSLOG\%COMPUTERNAME%_cert-User-IntermediateCA-GroupPolicy.txt
certutil -v -silent -user -store Disallowed >
c:\MSLOG\%COMPUTERNAME%_cert-User-UntrustedCertificates-
Registry.txt
certutil -v -silent -user -store -grouppolicy Disallowed >
c:\MSLOG\%COMPUTERNAME%_cert-User-UntrustedCertificates-
GroupPolicy.txt
certutil -v -silent -user -store AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-3rdPartyRootCA-Registry.txt
certutil -v -silent -user -store -grouppolicy AuthRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-3rdPartyRootCA-GroupPolicy.txt
certutil -v -silent -user -store SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-SmartCardRoot-Registry.txt
certutil -v -silent -user -store -grouppolicy SmartCardRoot >
c:\MSLOG\%COMPUTERNAME%_cert-User-SmartCardRoot-GroupPolicy.txt
certutil -v -silent -user -store UserDS >
c:\MSLOG\%COMPUTERNAME%_cert-User-UserDS.txt
```

- CA configuration information

Console

```
reg save HKLM\System\CurrentControlSet\Services\CertSvc
c:\MSLOG\%COMPUTERNAME%_CertSvc.hiv
reg export HKLM\System\CurrentControlSet\Services\CertSvc
c:\MSLOG\%COMPUTERNAME%_CertSvc.txt
reg save HKLM\SOFTWARE\Microsoft\Cryptography
c:\MSLOG\%COMPUTERNAME%_Cryptography.hiv
reg export HKLM\SOFTWARE\Microsoft\Cryptography
c:\MSLOG\%COMPUTERNAME%_Cryptography.txt
```

3. Copy the following files, if exist, to *C:\MSLOG: %windir%\CAPolicy.inf*

4. Sign in to a domain controller and create *C:\MSLOG* to store captured logs.

5. Launch Windows PowerShell as an administrator.

6. Run the following PowerShell cmdlets. Replace the domain name in ";.. ,DC=test,DC=local"; with appropriate domain name. The example shows commands for "; test.local"; domain.

   PowerShell

   ```
   Import-Module ActiveDirectory
   Get-ADObject -SearchBase ";CN=Public Key
   Services,CN=Services,CN=Configuration,DC=test,DC=local"; -Filter * -
   Properties * | fl * > C:\MSLOG\Get-ADObject_$Env:COMPUTERNAME.txt
   ```

7. Save the following logs.

   - All files in *C:\MSLOG* on the CA
   - All files in *C:\MSLOG* on the domain controller

Advanced troubleshooting 802.1X authentication

Article • 09/02/2022 • 4 minutes to read

Applies to: Windows 10

Overview

This article includes general troubleshooting for 802.1X wireless and wired clients. While troubleshooting 802.1X and wireless, it's important to know how the flow of authentication works, and then figure out where it's breaking. It involves many third-party devices and software. Most of the time, we have to identify where the problem is, and another vendor has to fix it. We don't make access points or switches, so it's not an end-to-end Microsoft solution.

Scenarios

This troubleshooting technique applies to any scenario in which wireless or wired connections with 802.1X authentication are attempted and then fail to establish. The workflow covers Windows 7 through Windows 10 (and Windows 11) for clients, and Windows Server 2008 R2 through Windows Server 2012 R2 for NPS.

Known issues

None

Data collection

See Advanced troubleshooting 802.1X authentication data collection.

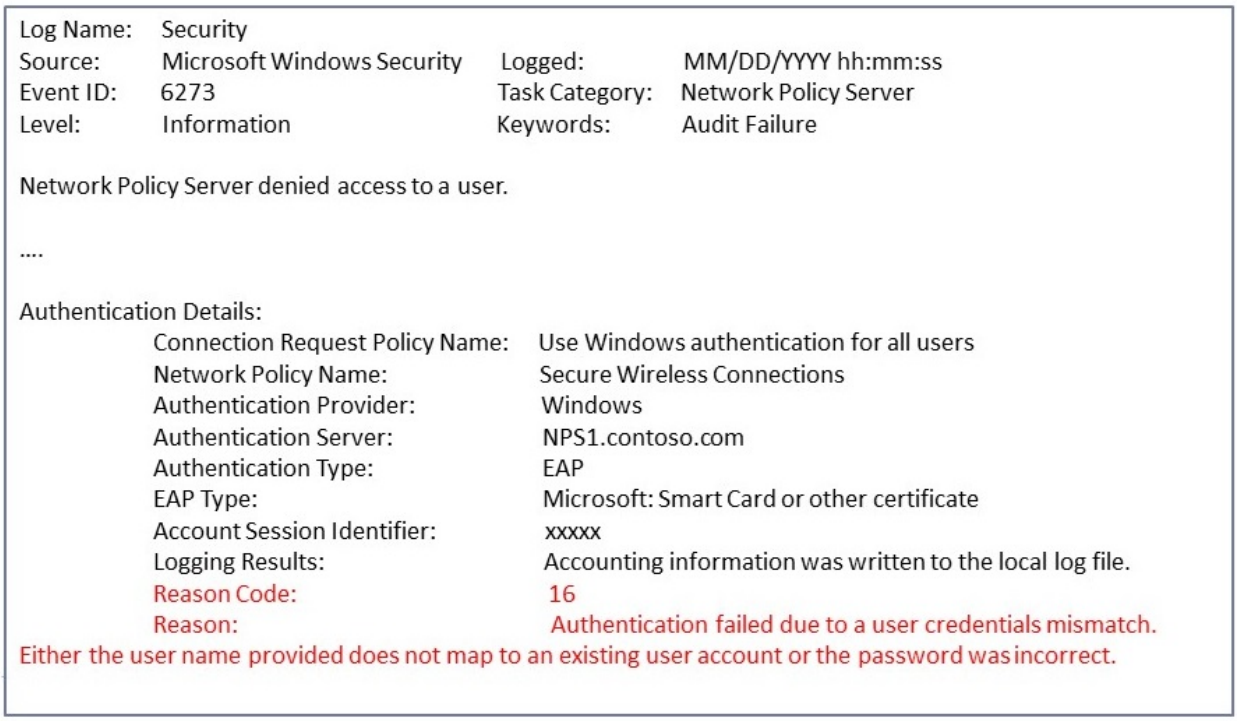
Troubleshooting

Viewing NPS authentication status events in the Windows Security event log is one of the most useful troubleshooting methods to obtain information about failed authentications.

NPS event log entries contain information about the connection attempt, including the name of the connection request policy that matched the connection attempt and the network policy that accepted or rejected the connection attempt. If you don't see both success and failure events, see the NPS audit policy section later in this article.

Check the Windows Security event log on the NPS Server for NPS events that correspond to the rejected (event ID 6273) or the accepted (event ID 6272) connection attempts.

In the event message, scroll to the bottom, and then check the Reason Code field and the text that's associated with it.



Example: event ID 6273 (Audit Failure)

Log Name: Security
Source: Microsoft Windows Security Logged: MM/DD/YYYY hh:mm:ss
Event ID: 6272 Task Category: Network Policy Server
Level: Information Keywords: Audit Success

Network Policy Server granted access to a user.

....

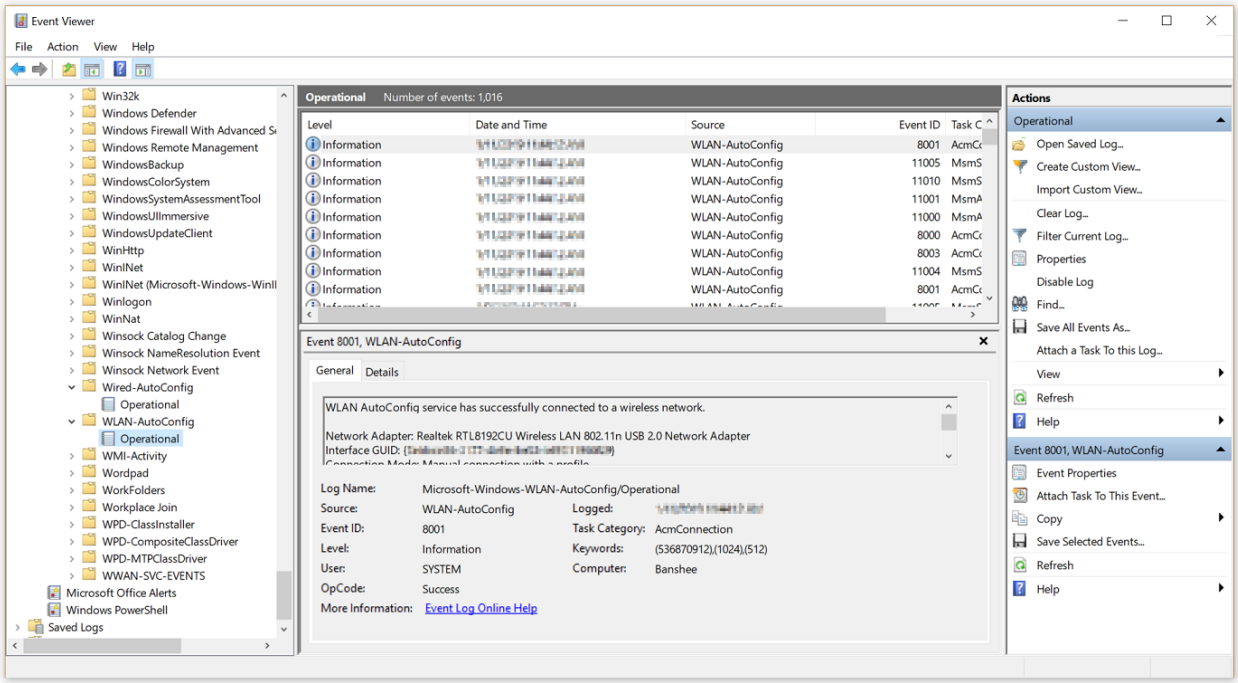
Authentication Details:

Connection Request Policy Name:	Use Windows authentication for all users
Network Policy Name:	Secure Wireless Connections
Authentication Provider:	Windows
Authentication Server:	NPS1.contoso.com
Authentication Type:	EAP
EAP Type:	Microsoft: Smart Card or other certificate
Account Session Identifier:	xxxxx
Logging Results:	Accounting information was written to the local log file.

Example: event ID 6272 (Audit Success)

The WLAN AutoConfig operational log lists information and error events based on conditions detected by or reported to the WLAN AutoConfig service. The operational log contains information about the wireless network adapter, the properties of the wireless connection profile, the specified network authentication, and, if connectivity problems occur, the reason for the failure. For wired network access, the Wired AutoConfig operational log is an equivalent one.

On the client side, go to *Event Viewer (Local)\Applications and Services Logs\Microsoft\Windows\WLAN-AutoConfig/Operational* for wireless issues. For wired network access issues, go to ..*Wired-AutoConfig/Operational*. See the following example:

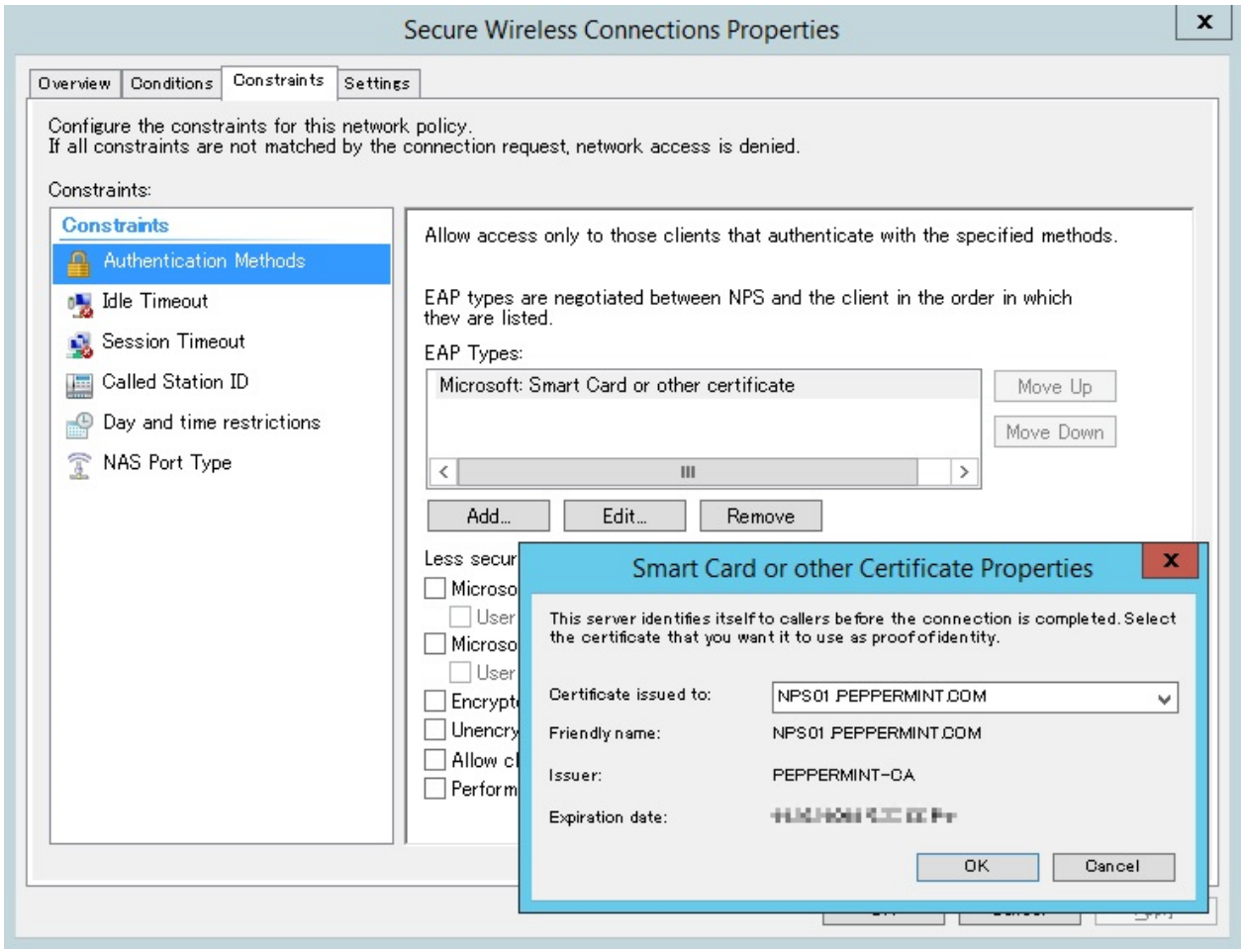


Most 802.1X authentication issues are because of problems with the certificate that's used for client or server authentication. Examples include invalid certificate, expiration, chain verification failure, and revocation check failure.

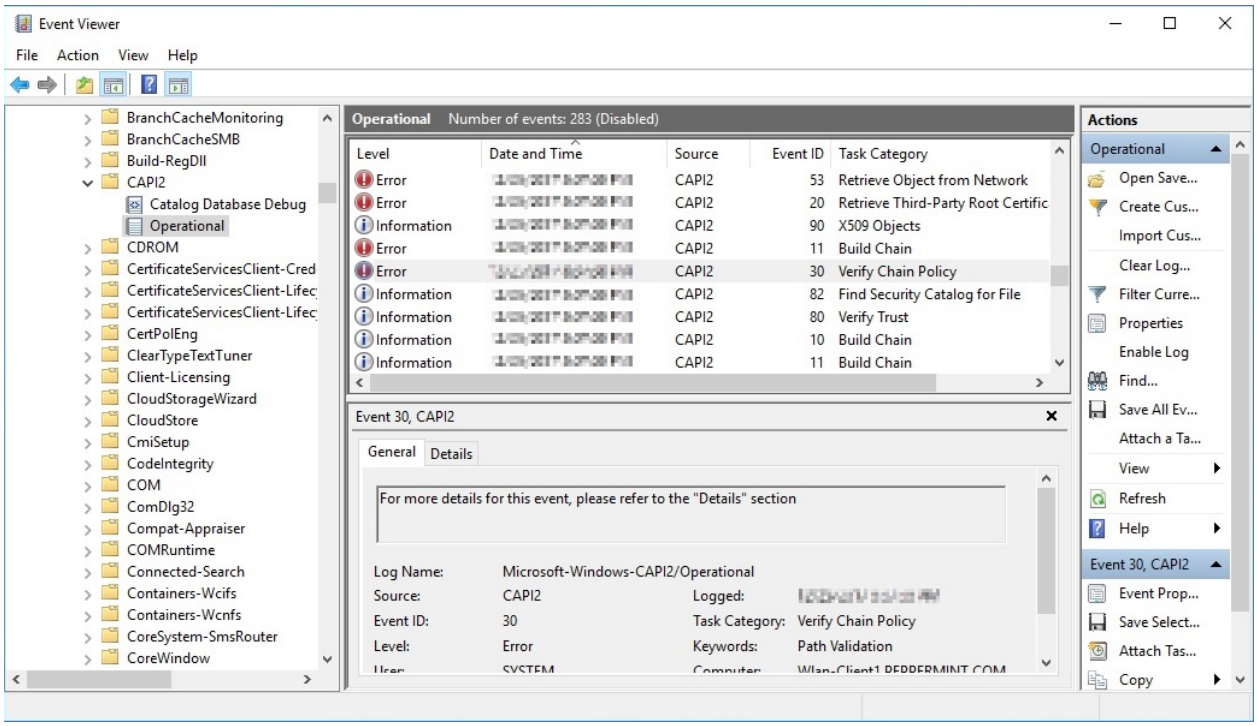
First, validate the type of EAP method that's used:

EAP Methods	Client Authentication Method	Server Authentication Method
EAP-MSCHAPv2	Username/Password	N/A
EAP-TLS	Certificate	Certificate
PEAP-MSCHAPv2	Username/Password	Certificate
PEAP-TLS	Certificate	Certificate

If a certificate is used for its authentication method, check whether the certificate is valid. For the server (NPS) side, you can confirm what certificate is being used from the EAP property menu. In **NPS snap-in**, go to **Policies** > **Network Policies**. Select and hold (or right-click) the policy, and then select **Properties**. In the pop-up window, go to the **Constraints** tab, and then select the **Authentication Methods** section.

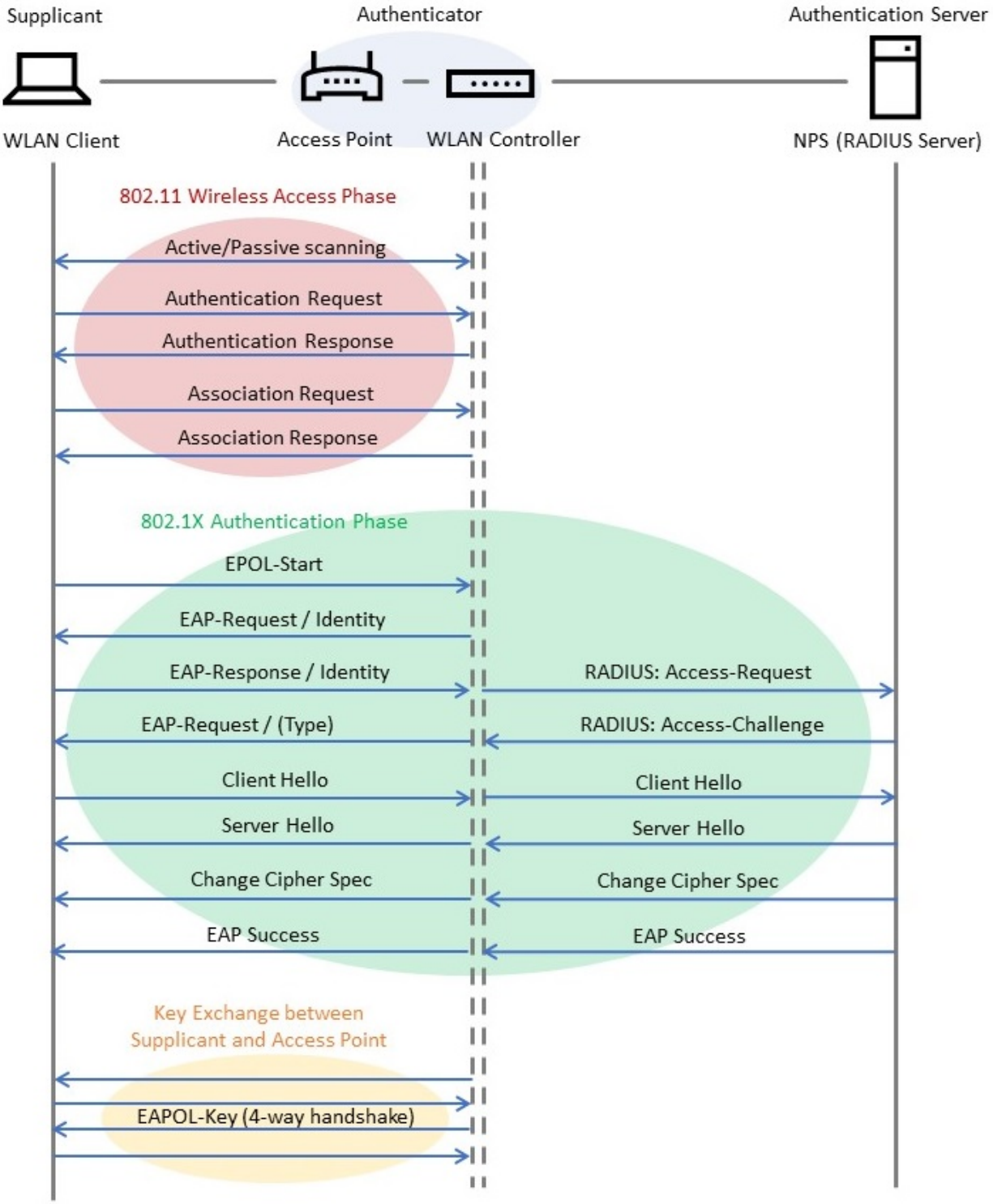


The CAPI2 event log is useful for troubleshooting certificate-related issues. By default, this log isn't enabled. To enable this log, expand *Event Viewer (Local)\Applications and Services Logs\Microsoft\Windows\CAPI2*, select and hold (or right-click) **Operational**, and then select **Enable Log**.

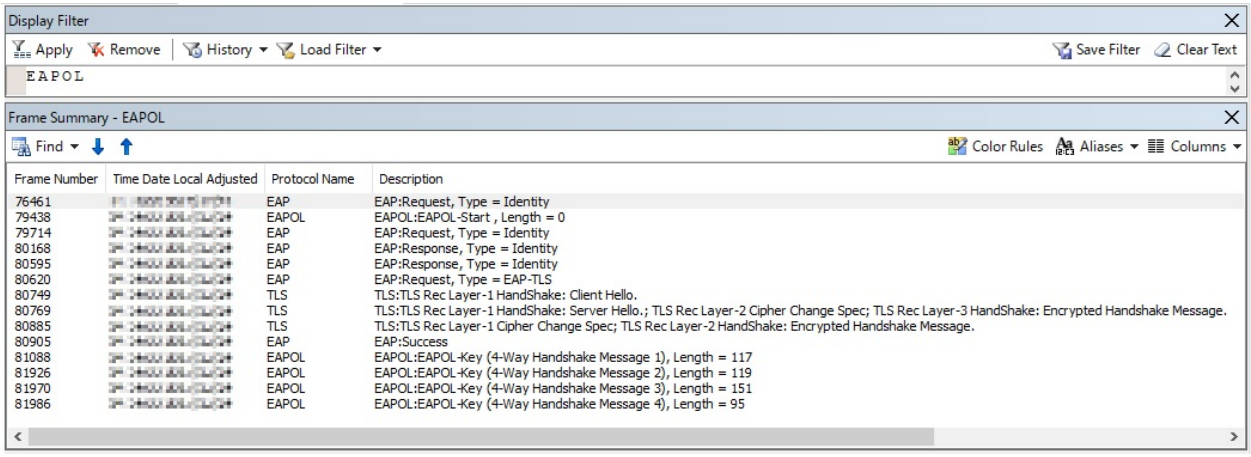


For information about how to analyze CAPI2 event logs, see Troubleshooting PKI Problems on Windows Vista.

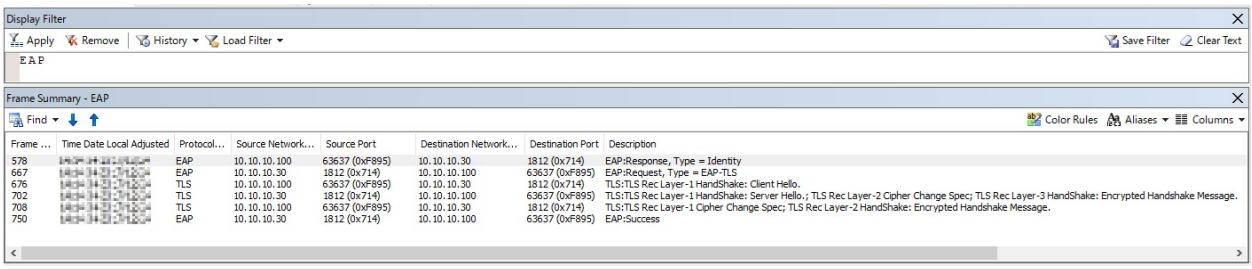
When troubleshooting complex 802.1X authentication issues, it's important to understand the 802.1X authentication process. Here's an example of wireless connection process with 802.1X authentication:



If you collect a network packet capture on both the client and the server (NPS) side, you can see a flow like the one below. Type *EAPOL* in the Display Filter for a client-side capture, and *EAP* for an NPS-side capture. See the following examples:

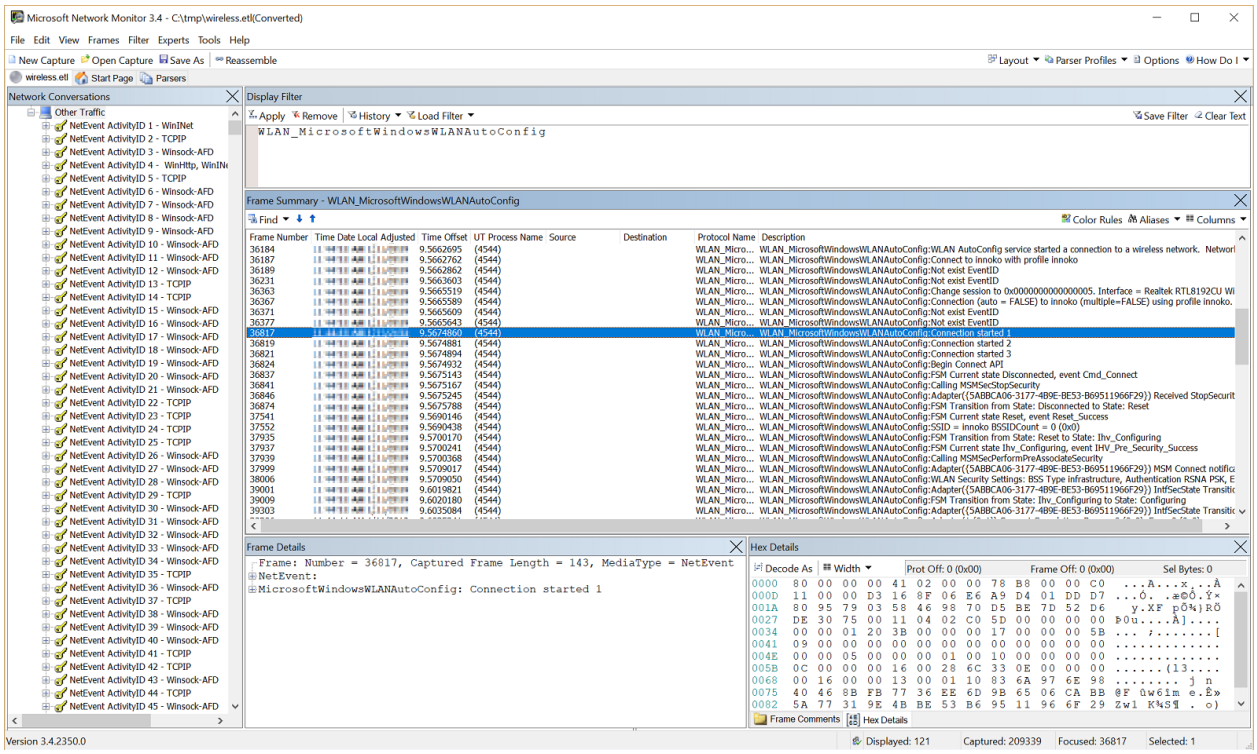


Client-side packet capture data



NPS-side packet capture data

> **ⓘ Note**
>
> If you have a wireless trace, you can also **view ETL files with network monitor** and apply the **ONEX_MicrosoftWindowsOneX** and **WLAN_MicrosoftWindowsWLANAutoConfig** Network Monitor filters. If you need to load the required **parser**, see the instructions under the **Help** menu in Network Monitor. Here's an example:



Audit policy

By default, NPS audit policy (event logging) for connection success and failure is enabled. If you find that one or both types of logging are disabled, use the following steps to troubleshoot.

View the current audit policy settings by running the following command on the NPS server:

Console

```
auditpol /get /subcategory:"Network Policy Server"
```

If both success and failure events are enabled, the output should be:

Output

```
System audit policy
Category/Subcategory                      Setting
Logon/Logoff
  Network Policy Server                   Success and Failure


If it says, "No auditing," you can run this command to enable it:

```console
auditpol /set /subcategory:"Network Policy Server" /success:enable
/failure:enable
```
```

Even if audit policy appears to be fully enabled, it sometimes helps to disable and then re-enable this setting. You can also enable Network Policy Server logon/logoff auditing by using Group Policy. To get to the success/failure setting, select **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Advanced Audit Policy Configuration** > **Audit Policies** > **Logon/Logoff** > **Audit Network Policy Server**.

More information

- Troubleshooting Windows Vista 802.11 Wireless Connections
- Troubleshooting Windows Vista Secure 802.3 Wired Connections

Code 31 error in Device Manager for WAN Miniport (Network monitor) device in Windows

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where Device Manager displays a yellow exclamation mark next to the WAN Miniport (Network monitor) device.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2871372

Symptoms

Consider the following scenario:

- You are installing Windows.
- You open Device Manager after the installation is complete.

In this scenario, Device Manager displays a yellow exclamation mark next to the WAN Miniport (Network monitor) device. Additionally, the **Details** tab of the device properties window displays the following message:

The device is not working properly because Windows cannot load the drivers required for this device. (Code 31)

Cause

This issue occurs because Windows cannot load the drivers that are required for the WAN (Network monitor) device. Because there is no driver associated with the device, it cannot be removed from Device Manager.

Resolution

To prevent this issue during future installs, you must integrate update 2822241 into the installation media that you use during setup.

For information about how to use Deployment Image Servicing and Management (DISM) to integrate a hotfix package into installation media, see Add or remove packages offline.

Workaround

If you have already installed the operating system and are currently receiving a "code 31" error on the WAN Miniport (Network Monitor) device, follow these steps:

1. Open Device Manager.
2. Right-click the WAN miniport (Network monitor) device, and then click **Update Driver Software**.
3. Click **Browse my computer for driver software**.
4. Click **Let me pick from a list of device drivers on my computer**.
5. Clear the **Show compatible hardware** check box.
6. In the column on the left side, select **Microsoft**, and in the column on the right side, select **Microsoft KM-TEST Loopback Adapter**.
7. In the **Update Driver Warning** dialog box, click **Yes** to continue installing this driver.
8. After the driver is installed, right-click the device, and then click **Uninstall**.
9. After the device is uninstalled, right-click the computer name in Device Manager, and then click **Scan for hardware changes**.
10. On the **View** menu, click **Show hidden devices**. The WAN Miniport (Network monitor) device should now be started and no longer have a yellow exclamation mark next to it.

How to configure Wi-Fi Sense and Paid Wi-Fi Services on Windows 10 in an enterprise

Article • 09/23/2021 • 2 minutes to read

This article discusses the methods to configure Wi-Fi Sense and Paid Wi-Fi Services in Windows 10.

Applies to: Windows 10 - all editions *Original KB number:* 3085719

Summary

Wi-Fi Sense can automatically make Wi-Fi connections on your computer so that you can go online quickly in more locations. Wi-Fi Sense can connect you to open Wi-Fi hotspots that are collected through crowdsourcing, or to Wi-Fi networks that your contacts share with you through Wi-Fi Sense.

Paid Wi-Fi Services enable you to get online by buying Wi-Fi at the hotspot through Microsoft Store. Windows will temporarily connect to open hotspots to see if paid Wi-Fi services are available.

More information

To disable Wi-Fi Sense and Paid Wi-Fi Services on computers in the enterprise, use the following methods, as appropriate for your device management process:

Configuring through the Windows Provisioning framework

Configuring through legacy Unattended Windows setup (if the enterprises use unattended setup for provisioning)

IT administrators can also use Group Policy to disable Wi-Fi Sense and Paid Wi-Fi Services.

For Windows 10 Version 1511 or later versions of Windows

Configure the Group Policy Object **Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering**

paid services under **Computer Configuration\Administrative Templates\Network\WLAN Service\WLAN Settings**.

For earlier versions of Windows than Windows 10 Version 1511

Configure the Group Policy to create and set the following DWORD registry value to **0** to disable Wi-Fi Sense:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WcmSvc\wifinetworkmanager\config\AutoConnectAllowedOEM`

> **Note**
>
> If you use Group Policy to disable Wi-Fi Sense, this also disables the following related Wi-Fi Sense features:

- Connect automatically to open hotspots
- Connect automatically to networks shared by my contacts
- Allow me to select networks to share my contacts

More information is available on TechNet: Registry Extension.

Event ID 10317 is logged when you turn on a mobile broadband device or resume it from sleep

Article • 09/23/2021 • 2 minutes to read

This article describes Event ID 10317 that's logged when you turn on a mobile broadband device or resume it from sleep.

Applies to: Windows 8.1
Original KB number: 2981681

Symptoms

You have a device that has a mobile broadband connection. When you turn on the device or resume it from sleep, one of the following errors is logged in the System log:

> Log Name: System
> Source: Microsoft-Windows-NDIS
> Date: <*Date and Time*>
> Event ID: 10317
> Task Category: PnP
> Level: Error
> Keywords: (16384),(16),(4),(2)
> User: <*User Name*>
> Computer: <*Computer Name*>
> Description:
> Miniport <*Mobile broadband device name*>, {*GUID*}, had event Fatal error: The miniport has detected an internal error

> Log Name: System
> Source: Microsoft-Windows-NDIS
> Date: <*Date and Time*>
> Event ID: 10317
> Task Category: PnP
> Level: Error
> Keywords: (16384),(16),(4),(2)
> User: <*User Name*>
> Computer: <*Computer Name*>

> Description:
> Miniport <*Mobile broadband device name*>, {*GUID*}, had event Fatal error: The miniport has failed a power transition to operational power

Cause

This error is logged when a request is sent to the mobile broadband device and a response is not received in 400 milliseconds. This frequently occurs when the mobile broadband device was turned off and is restarting. For example, this may occur during an initial start or when the device resumes from sleep or hibernation. In most cases, the device cannot start fast enough to be able to respond in the 400-millisecond window. After the device is fully turned on, these errors are typically no longer logged because the device is awake and able to respond quickly.

Resolution

These errors can safely be ignored when they are logged during or shortly after the device is turned on or resumed from sleep.

How to connect to a wireless network

Article • 12/06/2021 • 2 minutes to read

This article describes how to connect to a wireless network.

Applies to: Windows Vista
Original KB number: 928429

> **Note**
>
> Support for Windows Vista without any service packs installed ended on April 13, 2010. To continue receiving security updates for Windows, make sure you're running Windows Vista with Service Pack 2 (SP2). For more information, see this Microsoft web page: **Support is ending for some versions of Windows**

Introduction

This article describes how to connect to a wireless network in Windows Vista.

More information

The software that you were using together with Windows XP to connect to wireless networks is incompatible with Windows Vista. Alternatively, you can use Windows Vista to configure the wireless networks.

To connect to a wireless network in Windows Vista, follow these steps:

1. Click **Start** , and then click **Connect to**.
2. Click the wireless network to which you want to connect, and then click **Connect**.

> **Note**
>
> During the connection process, you may be prompted for a Wired Equivalent Privacy (WEP) key. If you do not have this key, contact the administrator of the wireless network for help.

For more information about how to connect to wireless networks by using Windows Vista, visit the following Microsoft Web site:
https://technet.microsoft.com/library/bb878035.aspx

For Wireless Wide Area Networks (2.5G/3G), the communication software is provided by the wireless carriers. Contact the IT manager of the company or call the wireless carrier that is providing the service for Windows Vista-compatible software.

Intel's My WiFi Technology stops working after resuming from sleep or hibernate in Windows 7

Article • 09/23/2021 • 2 minutes to read

This article provides help to fix an issue where Intel's My WiFi Technology stops working after your computer resumes from sleep or hibernate.

Applies to: Windows 7 Service Pack 1
Original KB number: 2560995

Symptoms

Consider the following scenario:

- You have Windows 7 installed on a notebook computer.
- The notebook computer has an Intel Wireless LAN device that supports Intel's My WiFi Technology (MWT).
- Within the Intel My Wifi Utility window, you select the Enable button.
- The computer enters sleep or hibernation.
- You wake the computer.

In this scenario, you may see the following status in the Intel My WiFi Utility window:

Disabled because the Hardware Radio Switch is Off. Turn on the hardware radio switch to enable Intel My WiFi Technology on your computer.

In addition, the Enable button is either not present or does not function. The expected behavior is that the Enable button should be available and functional within the application.

Cause

The above scenario may occur when the power management option " *Allow the computer to turn off this device to save power* " has been disabled for the Intel Wireless LAN device.

Resolution

You can work around this issue by using either of the two steps below:

- Enable the power management option "*Allow the computer to turn off this device to save power*" for the Intel Wireless LAN device using the following steps:

    1. Click on the **Start** button and select **Control Panel**.
    2. Select **System and Security**.
    3. Select **Device Manager** under **System**.
    4. Select and expand the **Network adapters** from the list of devices.
    5. Find the Intel Wireless LAN device and select it to bring up the **Properties** page.
    6. Select the **Power Management** tab.
    7. Under the **Power Management** tab, make sure the following option is checked (enabled): "*Allow the computer to turn off this device to save power*".

        > ⓘ **Note**
        >
        > If you have **Control Panel** configured to view by small or large icons, you may not see the **System and Security** category listed in step 2. In this case, select **System** from the available **Control Panel** applets and select **Device Manager** from the left pane. You can then skip steps 2 and 3 and continue with step 4.

- Alternatively, you can reboot your computer.

More information

More information on Intel's My WiFi Technology, including supported wireless networking adapters, can be obtained by visiting Intel's website.

Microsoft: Protected EAP (PEAP) option is missing while creating the Wireless Profile

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where Microsoft: Protected EAP (PEAP) option is missing in some cases.

Applies to: Windows 7 Service Pack 1
Original KB number: 2699785

Symptoms

There are multiple symptoms for the issue:

- Microsoft: Protected EAP (PEAP) option may be missing while creating the Wireless Profile on a client.
- Microsoft: Protected EAP (PEAP) option may go missing once we start file transfer using Window Easy Transfer wizard.
- Remote Access Connection Manager does not start.

Cause

The default location of the file SymRasMan.dll is %SystemRoot%\System32\rastls.dll. On installing Symantec Antivirus or Symantec Endpoint Protection the default location is then changed and edited in the registry to C:\Program Files\ Symantec\Symantec Endpoint Protection \SymRasMan.dll. After uninstallation this location is not reversed. The issue occurs because of a problem with registry keys that are not reverted to the defaults or .dll files indicated in registry values do not exist after removing Symantec Endpoint Protection 11.0.

These 2 registry hives are affected:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\25`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13`

The values of the following keys under EAP are modified from C:\System32\rastls.dll to C:\Program Files\Symantec\Symantec Endpoint Protection\SymRasMan.dll.

- ConfigUiPath
- IdentityPath
- InteractiveUIPath
- Path

4 new registry keys with their value as C:\Windows\ System32\rastls.dll are created.

- ConfigUiPathBack
- IdentityPathBack
- InteractiveUIPathBack
- PathBack

Resolution

> **ⓘ Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs.

To resolve this problem, modify the registry to correct the values of ConfigUiPath, IdentityPath, InteractiveUIPath and Path. To do this, follow these steps:

1. Click **Start**, click **Run**, type *regedit*, and then click **OK**.
2. Locate and then click the registry subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13`.
3. Select the folder 13.
4. Change the value for keys: ConfigUiPath, IdentityPath, InteractiveUIPath and Path to: C:\Windows\ System32\rastls.dll
5. Navigate to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\25`.
6. Select the folder 25.
7. Change the value for keys: ConfigUiPath, IdentityPath, InteractiveUIPath and Path to: C:\Windows\ System32\rastls.dll.

8. Delete the following keys under folder 13 and 25.

   Location:

   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\13`
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\25`

   Registry keys:

   - ConfigUiPathBack
   - IdentityPathBack
   - InteractiveUIPathBack
   - PathBack

9. Exist the registry editor and then restart the computer.

OpenGL applications do not run on a Miracast wireless display in Windows 10

Article • 09/23/2021 • 2 minutes to read

This article discusses an issue where OpenGL applications don't run on a Miracast wireless display in Windows 10.

Applies to: Windows 10 - all editions
Original KB number: 3083829

Symptoms

OpenGL applications do not run on Miracast wireless display in Windows 10. This problem occurs in the following Miracast configurations:

- Windows 10 is set to project in duplicate mode, and the Miracast display is set as the primary display.
- Windows 10 is set to project in extended mode, and the OpenGL application is on the Miracast display.
- Windows 10 is set to project in second screen-only mode, and the OpenGL application is on the Miracast display.

Cause

This problem occurs because the Miracast pipeline in Windows 10 does not yet support OpenGL applications on the Miracast video driver (MiraDisp.dll).

Status

Microsoft has confirmed that this is a problem.

Windows Security Alert appears when connecting to a wireless network on a workgroup machine

Article • 09/23/2021 • 2 minutes to read

This article helps fix an issue where a Windows Security alert appears when you connect to a wireless network on a workgroup machine.

Applies to: Windows 10 - all editions
Original KB number: 2518158

Symptoms

While connecting to a wireless network on a Windows system that is part of a workgroup, a Windows Security Alert dialog similar to the following may be displayed:

> The server `<Authentication server>` presented a valid certificate issued by `<CA name>`, but `<CA name>` is not configured as a valid trust anchor for this profile. Further, the server `<Authentication server>` is not configured as a valid NPS server to connect to this profile.

or

> The server `<Authentication server>` presented a valid certificate issued by `<CA name>`, but `<CA name>` is not configured as a valid trust anchor for this profile.

If you click the Connect button on the dialog box, the wireless connection will be established successfully.

Cause

To validate the server certificate, Windows will check if the second element in the chain, the Certification Authority (CA) that issued the end certificate, is a trusted CA for Windows NT Authentication. A CA is considered to be trusted if it exists in the `NTAuth` system registry store found in the `CERT_SYSTEM_STORE_LOCAL_MACHINE_ENTERPRISE` store location. If this verification fails, either of the warning messages in the Symptoms section

could occur. By default, the CA certificate is not in the NTAuth store on a Windows system that is part of a workgroup.

Resolution

To work around the issue, you can export the certificate of the CA that issued the certificate to the authentication server to a file. Copy the file to the workgroup machine and then run the following command from an elevated Command Prompt:

```
certutil -enterprise -addstore NTAuth CA_CertFilename.cer
```

More information

About How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store, please refer to https://support.microsoft.com/kb/295663

Virtual WiFi/SoftAP fails to start with error: The hosted network couldn't be started

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an error (The hosted network couldn't be started) that occurs when you start Virtual WiFi/SoftAP.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2625519

Symptoms

On Windows 7 and Windows Server 2008 R2, when you attempt to start Virtual WiFi/SoftAP you may receive the error: The hosted network couldn't be started.

Cause

This can occur if the "Allow the computer to turn off the device to save power" power option for the wireless network adapter is cleared.

Resolution

Enable the "Allow the computer to turn off the device to save power" power management option for the wireless network adapter using the following steps:

1. Click on the Start button and select Control Panel.
2. Select System and Security.
3. Select Device Manager under System.
4. Select and expand the Network adapters from the list of devices.
5. Find the wireless network adapter and right-click on it and select Properties.
6. Select the Power Management tab.
7. Under the Power Management tab, make sure the following option is checked (enabled): *Allow the computer to turn off this device to save power*.

Note: If you have Control Panel configured to view by small or large icons, you may not see the System and Security category listed in step 2. In this case, select System from the

available Control Panel applets and select Device Manager from the left pane. You can then skip steps 2-3 and continue with step 4.

More information

Microsoft Virtual WiFi/SoftAP is not supported on Windows 7/Windows Server 2008 R2 when this power option is disabled.

For more information about Virtual WiFi/SoftAP, see the following article:

About the Wireless Hosted Network

Wireless devices are disabled after you turn off Airplane mode

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where wireless devices are disabled after you turn off Airplane mode.

Applies to: Windows 10 - all editions
Original KB number: 2826798

Symptoms

Consider the following scenario:

- You have a computer that is running Windows 8.1 or Windows 8.
- You turn on Airplane mode to disable all wireless communication.
- You put the computer into Sleep or Hibernation mode, or you shut down the computer.
- You wake the computer from Sleep or Hibernation mode, or you restart the computer.
- You turn off Airplane mode to enable all wireless communication.

In this scenario, if you turn off Airplane mode before the wireless devices are initialized, the devices stay off even though Airplane mode is off.

Cause

This issue occurs because the Airplane mode setting changes before the wireless devices are configured. Therefore, the system cannot relay the Airplane mode settings to the devices.

Workaround

To work around this issue, follow these steps:

1. Swipe in from the right edge of the screen, or press the Windows logo key + C.
2. Tap or click **Settings**.
3. Tap or click **Change PC Settings**.
4. Tap or click **Wireless**.

5. Tap or click an affected device to turn it on again.

Windows clients performance troubleshooting documentation

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Performance-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Performance sub categories

- Applications
- Blue Screen/Bugcheck
- No Boot (not BugChecks)
- Performance monitoring tools
- Servicing
- Shutdown is slow or hangs
- Slow Performance

Applications freeze when they concurrently try to access a file on a network drive in Windows

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround to an issue in which applications freeze when they try to access the same file on a network drive in Windows.

Applies to: Windows 10 - all editions
Original KB number: 4039810

Symptoms

Consider the following scenario:

- You create a share folder on a server, and then you add a file to the folder.
- On a client that is running Windows 10, Windows 8.1, or Windows 7, you mount the shared folder as a network drive.
- You install third-party security software that includes a file system minifilter driver that is associated with an application.
- The minifilter is attached to both a local drive that holds the %SystemRoot% path (for example, a C drive) and the network drive for the shared folder that you created.
- The minifilter sends a message (by using the **FltSendMessage** function) that includes the file name in the network drive to the application.
- The application tries to open the file by using the file name that it receives.
- Another application on the same computer that is not associated with the minifilter tries to open the same file on the network drive at the same time.

In this scenario, both applications freeze.

Cause

This problem occurs because of a resource lock that is held by the Windows Client-Side Caching Driver (Csc.sys). When this issue occurs, Csc.sys gets a resource lock on a file, and then it requests a driver that's above it in a driver stack to open the file. This makes all applications that try to access the file wait. This also makes the minifilter's thread wait for its associated application to respond.

Workaround

If this problem has already occurred, restart the client.

To avoid this problem, disable **Offline Files** by using the **Local Group Policy Editor** (gpedit.msc). To do this, use the **Allow or disallow use of the Offline Files feature** Group Policy setting in **Computer Configuration\Administrative Templates\Network\Offline Files**.

> ⓘ **Note**
>
> If you have to use **Offline Files**, there is no workaround.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the beginning of the article.

More Information

It's generally a bad idea to hold locks across calls to the file system. The reason for this is documented in the following Developer Blog article:
Issuing IO in minifilters: Part 1 - FltCreateFile

To identify a minifilter that is attached to multiple drives as described in the "Symptoms" section, run the following commands at an administrative command prompt:

Console

```
fltmc instances -v C:

fltmc instances -v \Device\Mup
```

Check Point and Centrify applications stop working after the January 2017 Quality Update is installed

Article • 09/23/2021 • 2 minutes to read

This article describes an issue in which Check Point and Centrify applications stop working.

Applies to: Windows 10 - all editions
Original KB number: 4013396

Symptoms

Users who installed the January 2017 Quality Update for Windows 10 Version 1607 may experience an issue in which certain disk encryption and identity management applications from Check Point and Centrify no longer work.

More information

Temporary support from Microsoft to address this issue was introduced in the March 2017 Quality Update for Windows 10 Version 1607, and it will continue through June 2017.

This support is applicable only to Windows 10 Version 1607. For long-term support for Windows 10 Version 1607 and later versions, contact Check Point or Centrify about the availability of new, Windows-compatible versions of these applications.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Command prompt and PowerShell don't open after in-place upgrade of Windows 10 S

Article • 12/06/2021 • 2 minutes to read

This article provides a solution to an issue where Command prompt and PowerShell don't open after in-place upgrade of Windows 10 S.

Applies to: Windows 10, version 1809
Original KB number: 4019568

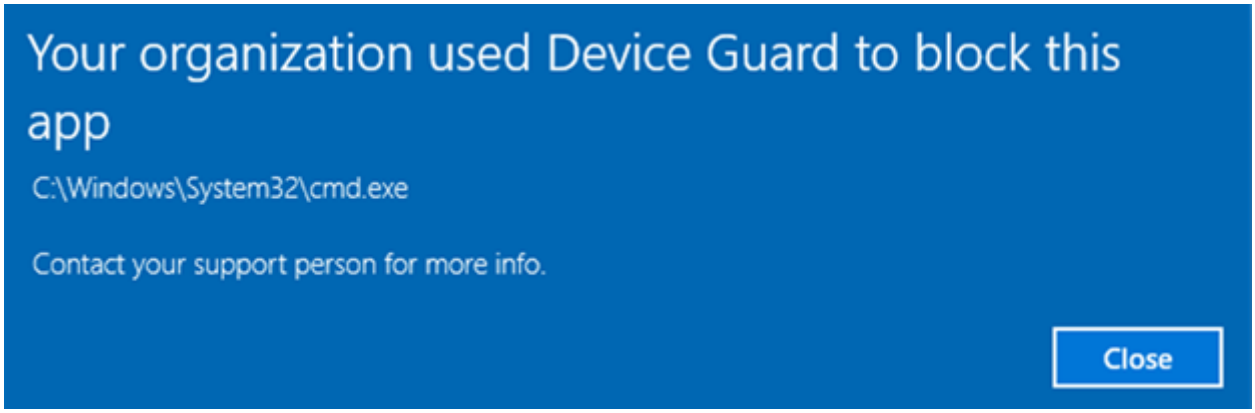
Symptom

Windows 10 S can be upgraded to Windows 10 Pro, Windows 10 Enterprise, or Windows 10 Education by using various methods. For example:

- Manually entering a product key
- Using Microsoft Store for Business
- Purchasing a license from the Microsoft Store
- Using installation media (in-place upgrade)

For more information, see Windows 10 edition upgrade Windows 10 edition upgrade.
After you do an in-place upgrade of Windows 10 S by using Setup.exe from Windows 10 installation media, when you open a command prompt, PowerShell, or any Win32 application, you may receive the following error message:
Your organization used Device Guard to block this app C:\Windows\System32\cmd.exe

Contact your support person for more info.



Cause

This issue occurs because the policy that allows Windows 10 S to control Win32 applications has not cleared.

Resolution

To resolve this issue, restart the computer. You may have to restart two or three times to clear this policy.

Reference

For more information about what is blocked in Windows 10 S, see Planning a Windows 10 in S mode deployment.

Error 1058 is displayed when a service suddenly stops

Article • 12/06/2021 • 2 minutes to read

This article provides a solution to an issue where "Error 1058" occurs when a service suddenly stops.

Applies to: Windows 10 - all editions, Windows 7, Windows Vista, Windows XP
Original KB number: 241584

Symptoms

When a service suddenly stops, you may receive the following error message:

> Error 1058: The service cannot be started, either because it is disabled or because it has no enabled devices associated with it.

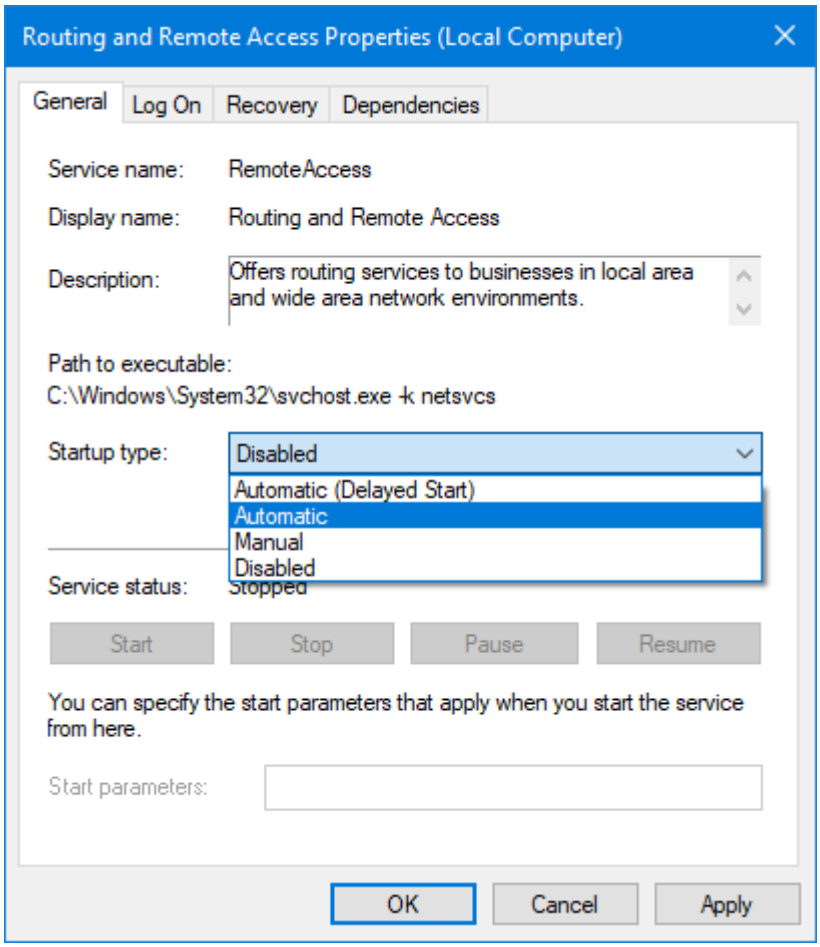
You may also receive this error message when you try to start a service.

Cause

This issue can occur if the service is disabled or if the service is disabled for the hardware profile that you're currently using.

Resolution for Windows 10, Windows 7 and Windows Vista

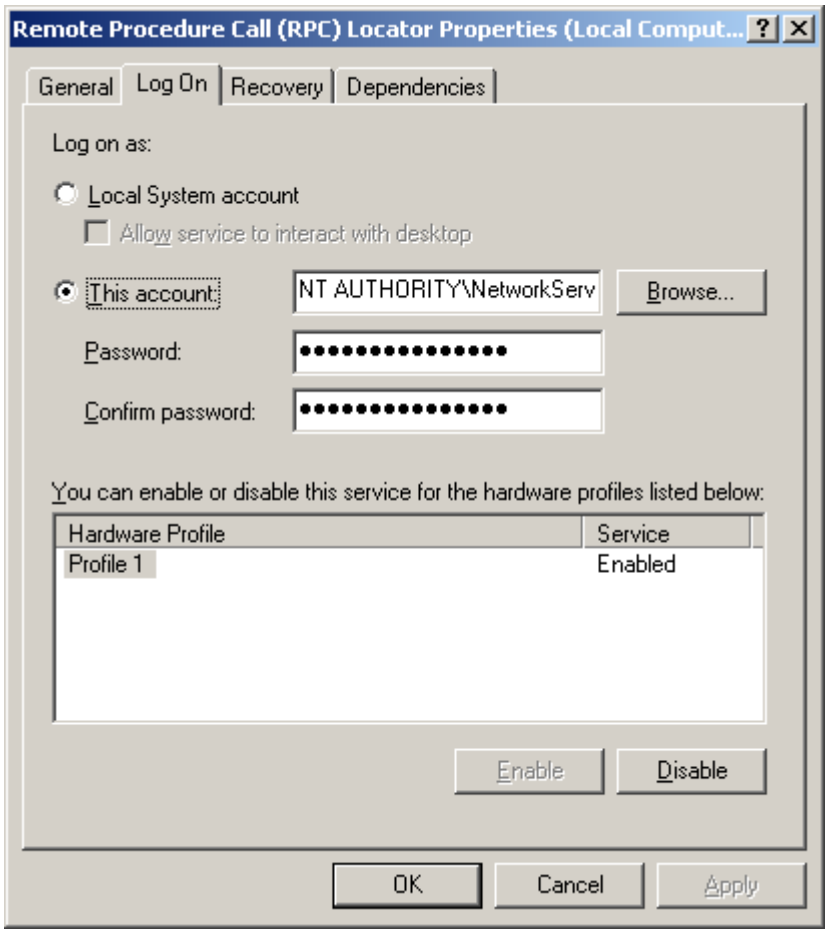
1. Click **Start**, search for *Services*, and then click **Services** in the search result.
2. Scroll until you find the service, and then double-click the service.



3. If the service is disabled, click the **Startup type** list, and then select an option other than **Disabled**.
4. Click **Apply**.
5. Click **Start** to try to start the service.
6. Click **OK**.

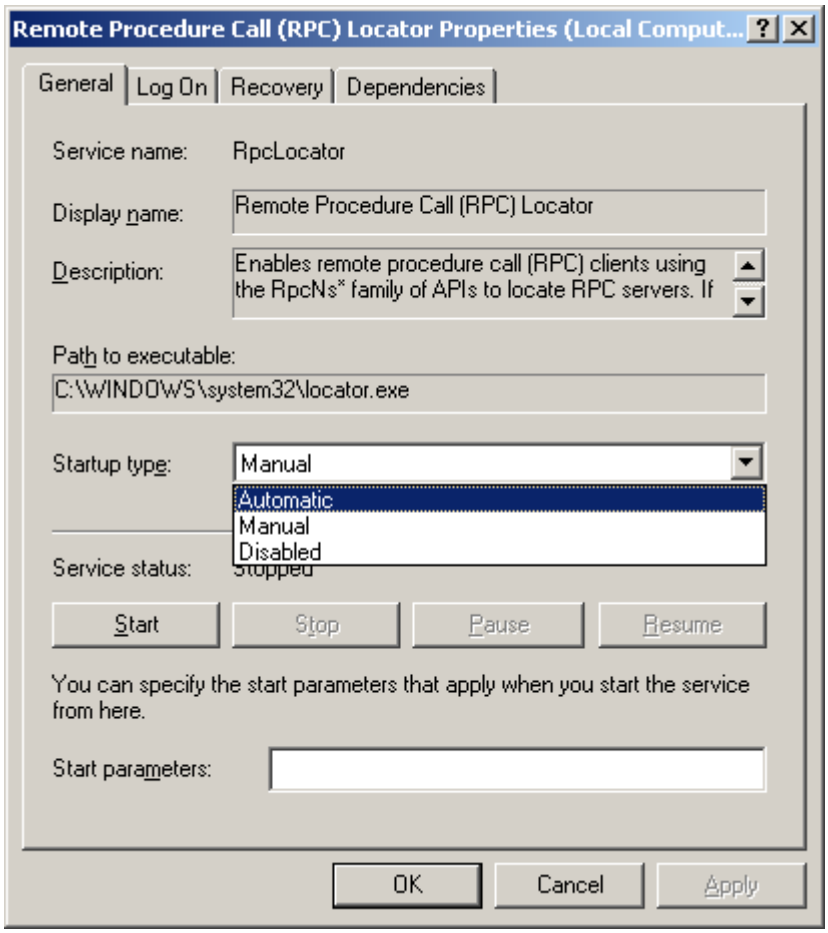
Resolution for Windows XP

1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Services**.
2. Scroll until you find the service that is stopped or disabled.
3. Double-click the service that did not start.
4. Click the **Log On** tab.



5. Verify that the service isn't disabled for the hardware profile that you're using. If the service is disabled for the hardware profile, click **Enable**.

6. Click the **General** tab, and then in the **Startup Type** box, verify that the service is not disabled. If the service is disabled, click **Automatic** to have it start when you start the computer.



7. Click **OK**.

More information

If a service is set to start automatically but the service is disabled for the hardware profile that you're using, the service isn't started and no error message is generated.

Flight Simulator X stops responding (hangs) on the loading screen

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where Microsoft Flight Simulator X stops responding on the loading screen.

Applies to: Windows 10 - all editions
Original KB number: 975084

Symptoms

When you start Flight Simulator X, the game stops responding (hangs) on the loading screen.

Resolution

To resolve this issue, rename the Logbook.bin file. To do this, follow these steps:

1. Click **Start**.
2. Click **My Documents** or **Documents**.
3. Double-click the Microsoft Flight Simulator X Files folder to open it.
4. Right-click the Logbook.bin file, and then click **Rename**.
5. Rename the file to *Logbook.OLD*, and then press ENTER.
6. Start Flight Simulator X to create a new Logbook file.

Memory allocation errors can be caused by slow page file growth

Article • 03/04/2022 • 2 minutes to read

This article provides a workaround for errors that occur when applications frequently allocate memory.

Applies to: Windows 10 - all editions
Original KB number: 4055223

Symptoms

Applications that frequently allocate memory may experience random "out-of-memory" errors. Such errors can result in other errors or unexpected behavior in affected applications.

Cause

Memory allocation failures can occur due to latencies that are associated with growing the size of a page file to support additional memory requirements in the system. A potential cause of these failures is when the page file size is configured as "automatic." Automatic page-file size starts with a small page file and grows automatically as needed.

The IO system consists of many components, including file system filters, file systems, volume filters, storage filters, and so on. The specific components on a given system can cause variability in page file growth.

Workaround

To work around this issue, manually configure the size of the page file. To do this, follow these steps:

1. Press the Windows logo key + the Pause/Break key to open **System Properties**.
2. Select **Advanced system settings** and then select **Settings** in the **Performance** section on the **Advanced** tab.
3. Select the **Advanced** tab, and then select **Change** in the **Virtual memory** section.
4. Clear the **Automatically manage paging file size for all drives** check box.
5. Select **Custom size**, and then set the "Initial size" and "Maximum size" values for the paging file. We recommend that you set the initial size to 1.5 times the amount

of RAM in the system.

6. Select **OK** to apply the settings, and then restart the system. If you continue to receive "out-of-memory" error messages, increase the "initial size" of the page file.

Status

Microsoft has confirmed that this is a problem in Windows 10.

More information

You might see intermittent build errors like the following if you encounter this problem when using the Microsoft Visual C++ compiler (cl.exe):

- Fatal error C1076: compiler limit: internal heap reached; use /Zm to specify a higher limit
- Fatal error C1083: cannot opentypefile: 'file': message
- Fatal error C1090: PDB API call failed, error code 'code': 'message'
- Compiler error C3859: virtual memory range for PCH exceeded; please recompile with a command line option of '-ZmXXX' or greater

For more information about the Visual C++ compiler errors and how to work around them, see Precompiled Header (PCH) issues and recommendations.

The file may start a different program when you run an .exe file in Windows 7

Article • 12/06/2021 • 2 minutes to read

This article provides a solution to an issue where the file may start a different program when you run an .exe file in Windows 7.

Applies to: Windows 7 Service Pack 1
Original KB number: 950505

Symptoms

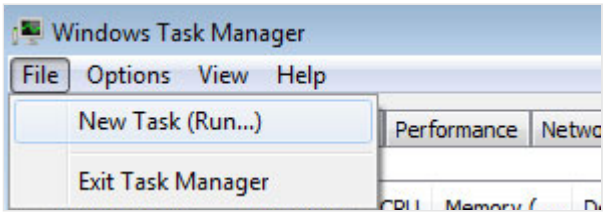
When you run an .exe file in Windows 7, the file may start a different program. Additionally, the icon for the .exe file may not appear as expected. You may also receive additional errors from the .exe file or from the program that starts.

Resolution

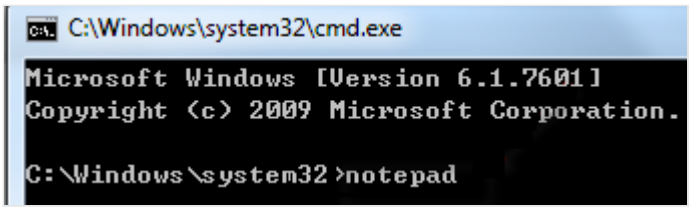
> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

To resolve this problem, reset the registry subkey for the file association of the .exe file back to the default setting. To do this, follow these steps:

1. To open the Task Manager, press CTRL + SHIFT + ESC.
2. Click **File**, press CTRL and click **New Task (Run...)** at the same time. A command prompt opens.



3. At the command prompt, type *notepad*, and then press ENTER.



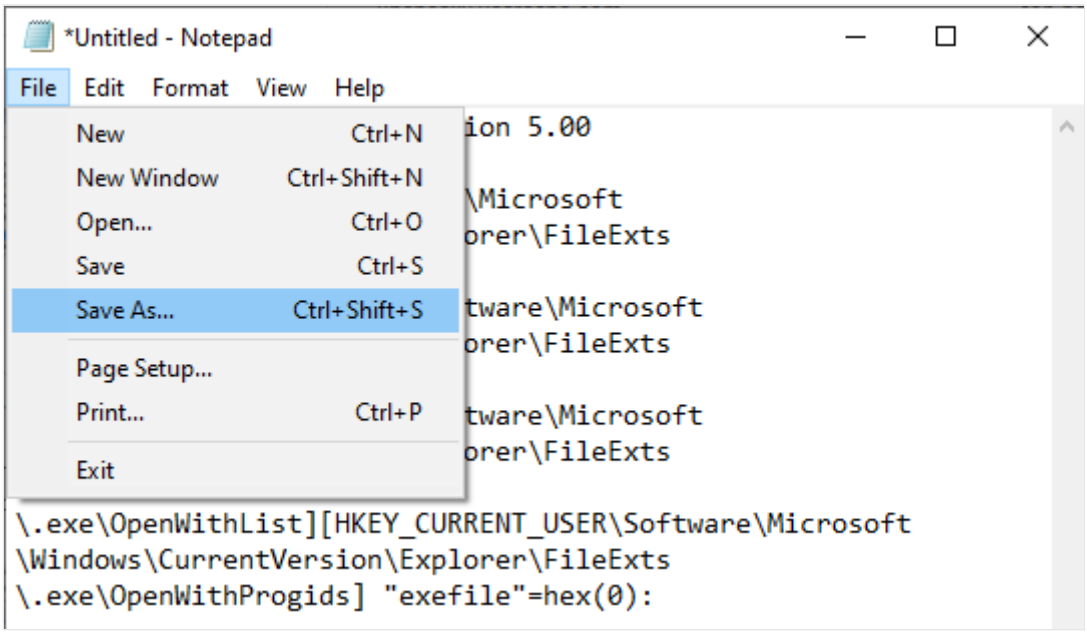
4. Paste the following text into Notepad:

```
Console

Windows Registry Editor Version 5.00

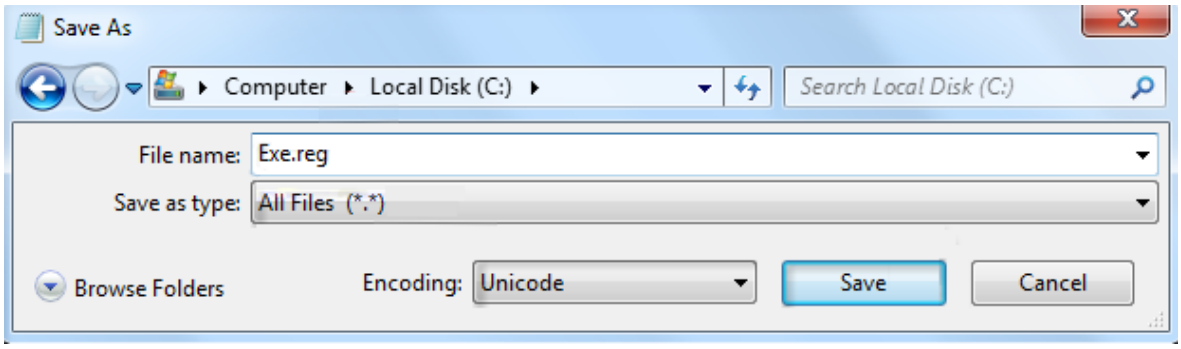
[-
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Fi
leExts\.exe]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\F
ileExts\.exe]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\F
ileExts\.exe\OpenWithList]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\F
ileExts\.exe\OpenWithProgids] "exefile"=hex(0):
```

5. On the **File** menu, click **Save as**.

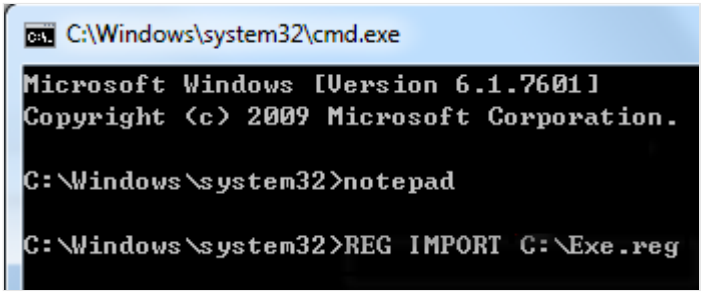


6. Select **All Files** in the **Save as type** list, and then type *Exe.reg* in the **File name** box.

7. Select **Unicode** in the **Encoding** list. Save it and remember the file location.



8. Return to the Command Prompt window, type `REG IMPORT <filepath> Exe.reg`, and then press ENTER.



> ⓘ Note
>
> <filepath> is a placeholder which is to input your Exe.reg file location (for example, C:\Exe.reg).

9. Click **Yes**, and then click **OK** in response to the registry prompts.
10. Log off from your account. Then, log back on to your account.

> ⓘ Note
>
> - You may have to restart the computer to restore the program icons to their original appearance.
> - After the problem is resolved, delete the Exe.reg file so that it is not mistakenly added back to the registry at a later date.

Some Windows procedures don't work if the Remote Procedure Call service is disabled

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where some Windows procedures don't work when the Remote Procedure Call (RPC) service is disabled.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 830071

> **Important**
>
> This article contains information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. For information about how to back up, restore, and edit the registry, see **Windows registry information for advanced users**.

Symptoms

When you restart your computer that runs Microsoft Windows NT 4.0, Microsoft Windows 2000, Microsoft Windows Server 2003, or Microsoft Windows XP, the following conditions may occur:

- You cannot move icons on the desktop.
- You cannot view event log entries.
- You can open the Services Microsoft Management Console (MMC), but you cannot see any services listed.

Cause

This problem may occur if you disable the RPC service. Many Windows operating system procedures depend on the RPC service.

Microsoft recommends that you don't disable the RPC service.

Resolution

> ⚠ **Warning**
>
> If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

To resolve this problem, follow these steps:

1. Click **Start,** click **Run**, type *regedt32*, and then click **OK**.
2. Expand the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcSs\`.
3. Double-click **Start**, type 2 in the **Edit DWORD Value** dialog box, and then click **OK**.
4. Close Registry Editor, and then restart your computer.

If your computer does not start correctly, you can use the Recovery Console to re-enable the RPC service. To use the Recovery Console, follow these steps:

1. Start your computer to the Recovery Console.
2. At the Recovery Console command prompt, type the `Enable RPCSS Service_Auto_Start` command, and then press ENTER.
3. At the Recovery Console command prompt, type `EXIT`, and then press ENTER.
4. Restart your computer.

More information

The following services depend on the RPC service:

- Background Intelligent Transfer Service
- COM+ Event System
- Distributed Link Tacking Client
- Distributed Transaction Coordinator
- Fax Service
- Indexing Service
- IPSec Policy Agent
- Messenger
- Network Connections
- Print Spooler
- Protected Storage

- Removable Storage
- Routing Information Protocol (RIP) Listener
- Routing and Remote Access
- Task Scheduler
- Telephony
- Telnet
- Windows Installer
- Windows Management Instrumentation

References

For more information about how to use the Recovery Console in Windows XP, in Windows 2000, or in Windows Server 2003, see What are the system recovery options in Windows? and How To Use the Recovery Console on a Windows Server 2003-Based Computer That Does Not Start.

SuperFetch(SysMain) service spikes the CPU for 1-2 minutes when a 64-bit application is running in Windows

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where the system experiences CPU spike for 1-2 minutes when a 64-bit application runs in the 64-bit version of Windows.

Applies to: Windows 7 Service Pack 1
Original KB number: 2723033

Symptoms

When a 64-bit application compiled with /LARGEADDRESSAWARE:NO option is running in the 64-bit versions of Windows, the system may experience CPU spike for 1-2 minutes and this goes on in-definitely. In this situation, the Task Manager shows the svchost.exe process hosting the SysMain(SuperFetch) service is consuming the CPU utilization.

Cause

Windows creates a single read-only Virtual Address Descriptor (VAD) for the address space above 2 GB while creating the process. SuperFetch while scanning the VAD tree of the running process encounters the VAD and spins with the huge VAD size, causing the CPU to spike.

Workaround

To work around this issue, avoid option /LARGEADDRESSAWARE:NO while compiling the applications.

> ⓘ **Note**
>
> By default a 64-bit application makes use of the Extended Address Space (8 terabytes per process).

Windows 10 causes issues when it calls CreateWindowEx in some 32-bit applications

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue in which Windows 10 causes issues when it calls CreateWindowEx in some 32-bit applications.

Applies to: Windows 10, version 1803, Windows 10, version 1709
Original KB number: 4054150

Symptoms

In some cases, the Windows 10 causes crashes or other issues when it calls the **CreateWindowEx** function in some 32-bit applications. We are aware of issues that affect some Microsoft Visual Studio extensions and the Bloomberg Professional service.

To determine whether your system is running Windows 10 Fall Creators Update (Version 1709, build 16299.19 or 16299.15), select **Start**, select **Settings**, select **System**, select **About**, and then look under **Windows specifications** for the Windows version information.

Workaround

To work around this issue, roll back your Windows 10 installation to the previous version.

The roll back option is available for 10 days after you've upgraded your Windows 10 installation. To roll back, select **Start**, select **Settings**, select **Update & Security**, and then select **Recovery**. This keeps your personal files, but removes applications and drivers that were installed after the upgrade, and also reverses any changes that you made to settings.

If the roll back option isn't available, please contact your IT support or helpdesk for help to restore the computer to the previous Window 10 version.

We recommend that you make a backup of your personal files before you contact your IT support, helpdesk, or Microsoft Support.

Status

Microsoft is working on a resolution and will provide an update in an upcoming release.

References

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Advanced troubleshooting for Event ID 41: "The system has rebooted without cleanly shutting down first"

Article • 10/25/2022 • 6 minutes to read

> **Note**
>
> Home users: This article is intended for use by support agents and IT professionals. If you're looking for more information about blue screen error messages, please visit **Troubleshoot blue screen errors**.

The preferred way to shut down Windows is to select **Start**, and then select an option to turn off or shut down the computer. When you use this standard method, the operating system closes all files and notifies the running services and applications so that they can write any unsaved data to disk and flush any active caches.

If your computer shuts down unexpectedly, Windows logs Event ID 41 the next time that the computer starts. The event text resembles the following information:

Output

```
Event ID: 41
Description: The system has rebooted without cleanly shutting down first.
```

This event indicates that some unexpected activity prevented Windows from shutting down correctly. Such a shutdown might be caused by an interruption in the power supply or by a Stop error. If feasible, Windows records any error codes as it shuts down. During the kernel phase of the next Windows startup, Windows checks for these codes and includes any existing codes in the event data of Event ID 41.

Output

```
EventData
BugcheckCode 159
BugcheckParameter1 0x3
BugcheckParameter2 0xfffffa80029c5060
BugcheckParameter3 0xfffff8000403d518
BugcheckParameter4 0xfffffa800208c010
SleepInProgress false
PowerButtonTimestamp 0Converts to 0x9f (0x3, 0xfffffa80029c5060,
0xfffff8000403d518, 0xfffffa800208c010)
```

How to use Event ID 41 when you troubleshoot an unexpected shutdown or restart

By itself, Event ID 41 might not contain sufficient information to explicitly define what occurred. Typically, you've to also consider what was occurring at the time of the unexpected shutdown (for example, the power supply failed). Use the information in this article to identify a troubleshooting approach that is appropriate for your circumstances:

- Scenario 1: The computer restarts because of a Stop error, and Event ID 41 contains a Stop error (bug check) code
- Scenario 2: The computer restarts because you pressed and held the power button
- Scenario 3: The computer is unresponsive or randomly restarts, and Event ID 41 isn't logged or the Event ID 41 entry lists error code values of zero

Scenario 1: The computer restarts because of a Stop error, and Event ID 41 contains a Stop error (bug check) code

When a computer shuts down or restarts because of a Stop error, Windows includes the Stop error data in Event ID 41 as part of more event data. This information includes the Stop error code (also called a bug check code), as shown in the following example:

Output

```
EventData
BugcheckCode 159
BugcheckParameter1 0x3
BugcheckParameter2 0xfffffa80029c5060
BugcheckParameter3 0xfffff8000403d518
BugcheckParameter4 0xfffffa800208c010
```

Note

Event ID 41 includes the bug check code in decimal format. Most documentation that describes bug check codes refers to the codes as hexadecimal values instead of decimal values. To convert decimal to hexadecimal, follow these steps:

1. Select **Start**, type *calc* in the **Search** box, and then select **Calculator**.
2. In the **Calculator** window, select **View** > **Programmer**.
3. On the left side of calculator, verify that **Dec** is highlighted.
4. Use the keyboard to enter the decimal value of the bug check code.

5. On the left side of the calculator, select **Hex**.

   The value that the calculator displays is now the hexadecimal code.

When you convert a bug check code to hexadecimal format, verify that the "0x" designation is followed by eight digits (that is, the part of the code after the "x" includes enough zeros to fill out eight digits). For example, 0x9F is typically documented as 0x0000009f, and 0xA is documented as 0x0000000A. In the case of the example event data in this article, "159" converts to 0x0000009f.

After you identify the hexadecimal value, use the following references to continue troubleshooting:

- Advanced troubleshooting for Stop error or blue screen error issue.
- Bug Check Code Reference. This page lists links to documentation for different bug check codes.
- How to Debug Kernel Mode Blue Screen Crashes (for beginners).

Scenario 2: The computer restarts because you pressed and held the power button

Because this method of restarting the computer interferes with the Windows shutdown operation, we recommend that you use this method only if you've no alternative. For example, you might have to use this approach if your computer isn't responding. When you restart the computer by pressing and holding the power button, the computer logs an Event ID 41 that includes a non-zero value for the **PowerButtonTimestamp** entry.

For help when troubleshooting an unresponsive computer, see Windows Help. Consider searching for assistance by using keywords such as "hang," "responding," or "blank screen."

Scenario 3: The computer is unresponsive or randomly restarts, and Event ID 41 isn't recorded or the Event ID 41 entry or lists error code values of zero

This scenario includes the following circumstances:

- You shut off power to an unresponsive computer, and then you restart the computer.
  To verify that a computer is unresponsive, press the `Caps lock` key on the keyboard. If the `Caps lock` light on the keyboard doesn't change when you press

the `Caps lock` key, the computer might be unresponsive (also known as a hard hang).
- The computer restarts, but it doesn't generate Event ID 41.
- The computer restarts and generates Event ID 41, but the **BugcheckCode** and **PowerButtonTimestamp** values are zero.

In such cases, something prevents Windows from generating error codes or from writing error codes to disk. Something might block write access to the disk (as in the case of an unresponsive computer) or the computer might shut down too quickly to write the error codes or even detect an error.

The information in Event ID 41 provides some indication of where to start checking for problems:

- Event ID 41 isn't recorded or the bug check code is zero. This behavior might indicate a power supply problem. If the power to a computer is interrupted, the computer might shut down without generating a Stop error. If it does generate a Stop error, it might not finish writing the error codes to disk. The next time the computer starts, it might not log Event ID 41. Or, if it does, the bug check code is zero. The following conditions might be the cause:
  - In the case of a portable computer, the battery was removed or drained.
  - In the case of a desktop computer, the computer was unplugged or experienced a power outage.
  - The power supply is underpowered or faulty.

- The PowerButtonTimestamp value is zero. This behavior might occur if you disconnected the power to a computer that wasn't responding to input. The following conditions might be the cause:
  - A Windows process blocked write access to the disk, and you shut down the computer by pressing and holding the power button for at least four seconds.
  - You disconnected the power to an unresponsive computer.

Typically, the symptoms described in this scenario indicate a hardware problem. To help isolate the problem, do the following steps:

- Disable overclocking. If the computer has overclocking enabled, disable it. Verify that the issue occurs when the system runs at the correct speed.
- Check the memory. Use a memory checker to determine the memory health and configuration. Verify that all memory chips run at the same speed and that every chip is configured correctly in the system.
- Check the power supply. Verify that the power supply has enough wattage to appropriately handle the installed devices. If you added memory, installed a newer processor, installed more drives, or added external devices, such devices can

require more energy than the current power supply can provide consistently. If the computer logged Event ID 41 because the power to the computer was interrupted, consider obtaining an uninterruptible power supply (UPS) such as a battery backup power supply.

- Check for overheating. Examine the internal temperature of the hardware and check for any overheating components.

If you perform these checks and still can't isolate the problem, set the system to its default configuration and verify whether the issue still occurs.

> **Note**
>
> If you see a Stop error message that includes a bug check code, but Event ID 41 doesn't include that code, change the restart behavior for the computer. To do this, follow these steps:
>
> 1. Right-click **My Computer**, then select **Properties** > **Advanced system settings** > **Advanced**.
> 2. In the **Startup and Recovery** section, select **Settings**.
> 3. Clear the **Automatically restart** check box.

Advanced troubleshooting for Stop error 7B or Inaccessible_Boot_Device

Article • 09/02/2022 • 8 minutes to read

This article provides steps to troubleshoot "Stop error 7B: Inaccessible_Boot_Device". This error might occur after some changes are made to the computer, or immediately after you deploy Windows on the computer.

Applies to: Windows 10

Causes of the Inaccessible_Boot_Device stop error

Any one of the following factors might cause the stop error:

- Missing, corrupted, or misbehaving filter drivers that are related to the storage stack
- File system corruption
- Changes to the storage controller mode or settings in the BIOS
- Using a different storage controller than the one that was used when Windows was installed
- Moving the hard disk to a different computer that has a different controller
- A faulty motherboard or storage controller, or faulty hardware
- In unusual cases, the failure of the TrustedInstaller service to commit newly installed updates is because of component-based store corruptions
- Corrupted files in the Boot partition (for example, corruption in the volume that's labeled **SYSTEM** when you run the `diskpart` > `list vol` command)
- If there's a blank GPT entry before the entry of the Boot partition

Troubleshoot this error

Start the computer in Windows Recovery Mode (WinRE) by following these steps.

1. Start the system by using the installation media for the installed version of Windows.
2. On the **Install Windows** screen, select **Next** > **Repair your computer**.
3. On the **System Recovery Options** screen, select **Next** > **Command Prompt**.

Verify that the boot disk is connected and accessible

Step 1

At the WinRE Command prompt, run `diskpart`, and then run `list disk`.

A list of the physical disks that are attached to the computer should be displayed and resemble the following display:

Console

```
  Disk ###  Status         Size     Free     Dyn  Gpt

  --------  -------------  -------  -------  ---  ---

  Disk 0    Online         **size*  GB      0 B        *
```

If the computer uses a Unified Extensible Firmware Interface (UEFI) startup interface, there will be an asterisk *() in the *GPT* column.

If the computer uses a basic input/output system (BIOS) interface, there won't be an asterisk in the **Dyn** column.

Step 2

If the `list disk` command lists the OS disks correctly, run the `list vol` command in `diskpart`.

`list vol` generates an output that resembles the following display:

Console

```
  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info

  ----------  ---  -----------  -----  ----------  -------  ---------  -----
---

  Volume 0         Windows RE   NTFS   Partition    499 MB  Healthy

  Volume 1     C   OSDisk       NTFS   Partition    222 GB  Healthy    Boot

  Volume 2         SYSTEM       FAT32  Partition    499 MB  Healthy
System
```

ⓘ Note

If the disk that contains the OS isn't listed in the output, you'll have to engage the OEM or virtualization manufacturer.

Verify the integrity of Boot Configuration Database

Check whether the Boot Configuration Database (BCD) has all the correct entries. To do this step, run `bcdedit` at the WinRE command prompt.

To verify the BCD entries:

1. Examine the **Windows Boot Manager** section that has the **{bootmgr}** identifier. Make sure that the **device** and **path** entries point to the correct device and boot loader file.

   If the computer is UEFI-based, here's example output:

   ```
   Console

   device                  partition=\Device\HarddiskVolume2
   path                    \EFI\Microsoft\Boot\bootmgfw.efi
   ```

   If the machine is BIOS-based, here's example output:

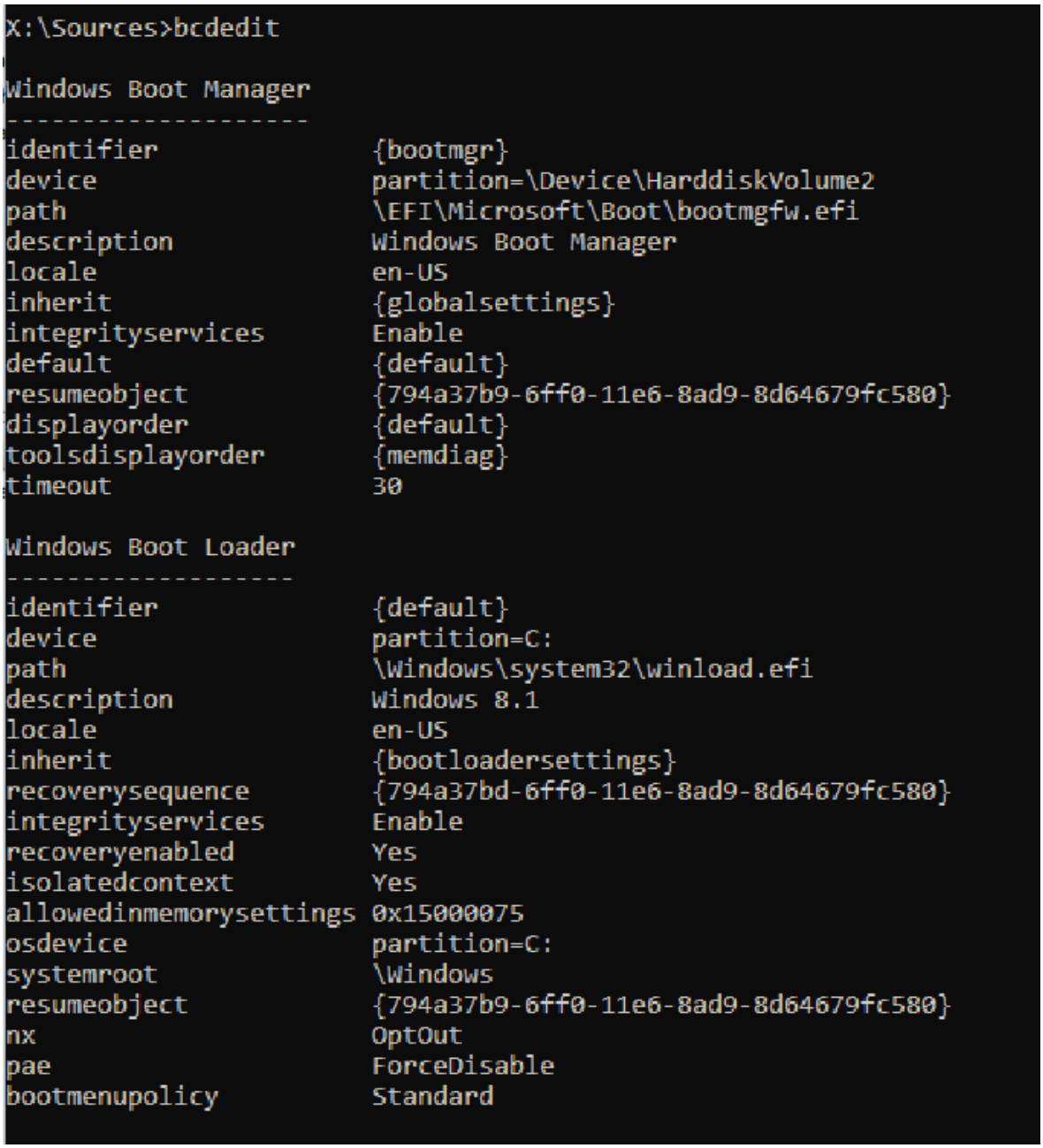
   ```
   Console

   Device                  partition=C:
   ```

   > **Note**
   >
   > This output might not contain a path.

2. In the **Windows Boot Loader** that has the **{default}** identifier, make sure that **device**, **path**, **osdevice**, and **systemroot** point to the correct device or partition, winload file, OS partition or device, and OS folder.

   > **Note**
   >
   > If the computer is UEFI-based, the file path value that's specified in the **path** parameter of **{bootmgr}** and **{default}** contains an **.efi** extension.



If any of the information is wrong or missing, we recommend that you create a backup of the BCD store. To do this, run `bcdedit /export C:\temp\bcdbackup`. This command creates a backup in *C:\temp* that's named **bcdbackup**. To restore the backup, run `bcdedit /import C:\temp\bcdbackup`. This command overwrites all BCD settings by using the settings in **bcdbackup**.

After the backup completes, run the following command to make the changes:

Console

```
bcdedit /set *{identifier}* option value
```

For example, if the device under {default} is wrong or missing, run this command to set it: `bcdedit /set {default} device partition=C:`

If you want to completely re-create the BCD, or if you get a message that states that "**The boot configuration data store could not be opened. The system could not find the file specified,** " run `bootrec /rebuildbcd`.

If the BCD has the correct entries, check whether the **winload** and **bootmgr** entries exist in the correct location, which is in the specified path in the **bcdedit** command. By default, **bootmgr** in the BIOS partition is in the root of the **SYSTEM** partition. To see the file, run `Attrib -s -h -r`.

If the files are missing, and you want to rebuild the boot files, follow these steps:

1. Copy all the contents under the **SYSTEM** partition to another location. Alternatively, you can use the command prompt to navigate to the OS drive, create a new folder, and then copy all the files and folders from the **SYSTEM** volume, like shown here:

   Console

   ```
   D:\> Mkdir  BootBackup
   R:\> Copy *.* D:\BootBackup
   ```

2. If you're using Windows 10, or if you're troubleshooting by using a Windows 10 ISO at the Windows Pre-Installation Environment command prompt, you can use the `bcdboot` command to re-create the boot files, like shown here:

   Console

   ```
   Bcdboot <**OSDrive* >:\windows /s <**SYSTEMdrive* >: /f ALL
   ```

   For example, if we assign the `<System Drive>` (WinRE drive) the letter R and the `<OSdrive>` is the letter D, we would use the following command:

   Console

   ```
   Bcdboot D:\windows /s R: /f ALL
   ```

   > ⓘ **Note**
   >
   > The **ALL** part of the `bcdboot` command writes all the boot files (both UEFI and BIOS) to their respective locations.

If you don't have a Windows 10 ISO, format the partition and copy **bootmgr** from another working computer that has a similar Windows build. To do the formatting and copying, follow these steps:

1. Start **Notepad**.
2. Press Ctrl+O.
3. Navigate to the system partition (in this example, it's R).
4. Right-click the partition, and then format it.

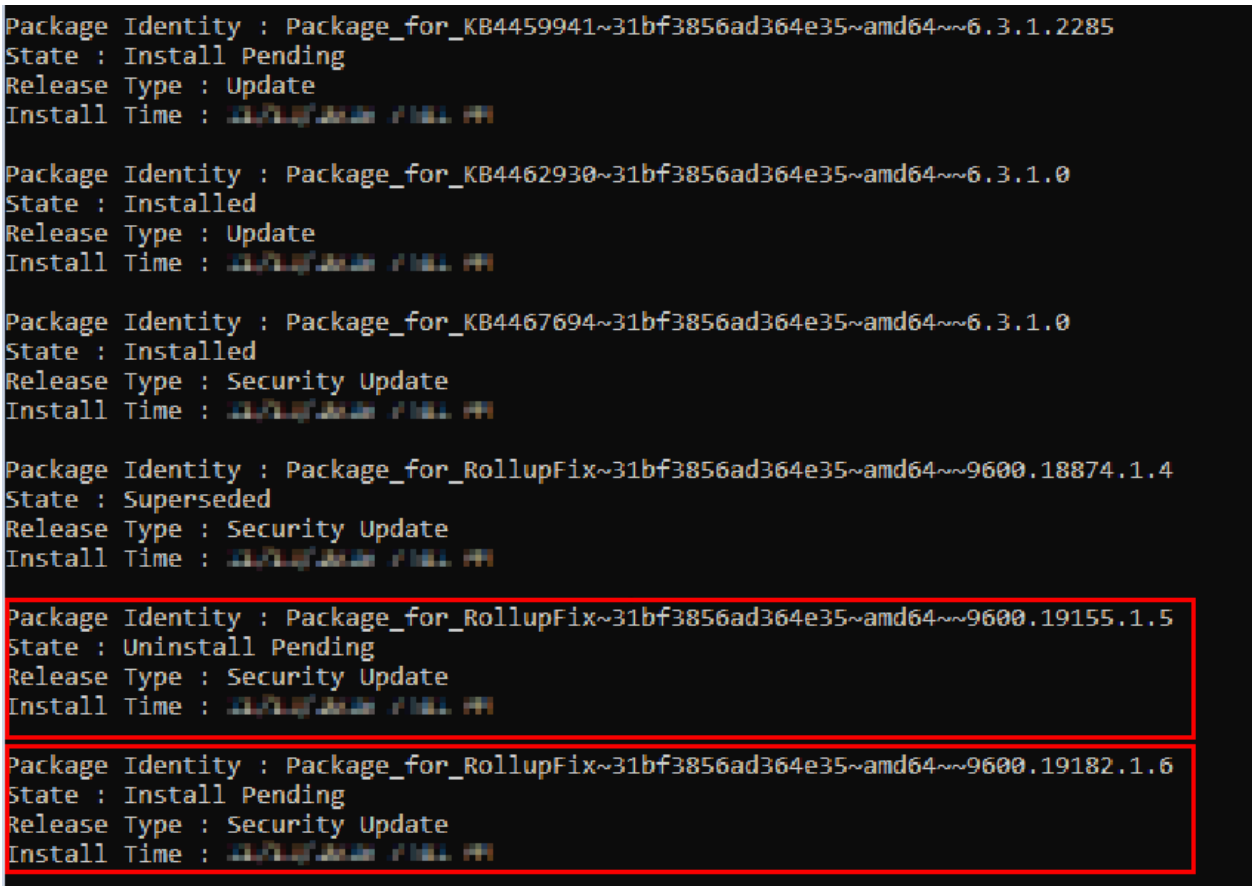
Troubleshooting if this issue occurs after a Windows Update installation

Run the following command to verify the Windows update installation and dates:

```
Console

Dism /Image:<Specify the OS drive>: /Get-packages
```

After you run this command, you'll see the **Install pending** and **Uninstall Pending** packages:



1. Run the `dism /Image:C:\ /Cleanup-Image /RevertPendingActions` command.

   Replace C: with the system partition for your computer.

```
X:\Sources>dism /Image:C:\ /Cleanup-Image /RevertPendingActions

Deployment Image Servicing and Management tool
Version: 10.0.17134.1

Image Version: 6.3.9600.17709

The scratch directory size might be insufficient to perform this operation. This can cause unexpected behavior.
Use the /ScratchDir option to point to a folder with sufficient scratch space. The recommended size is at least 1024 MB.

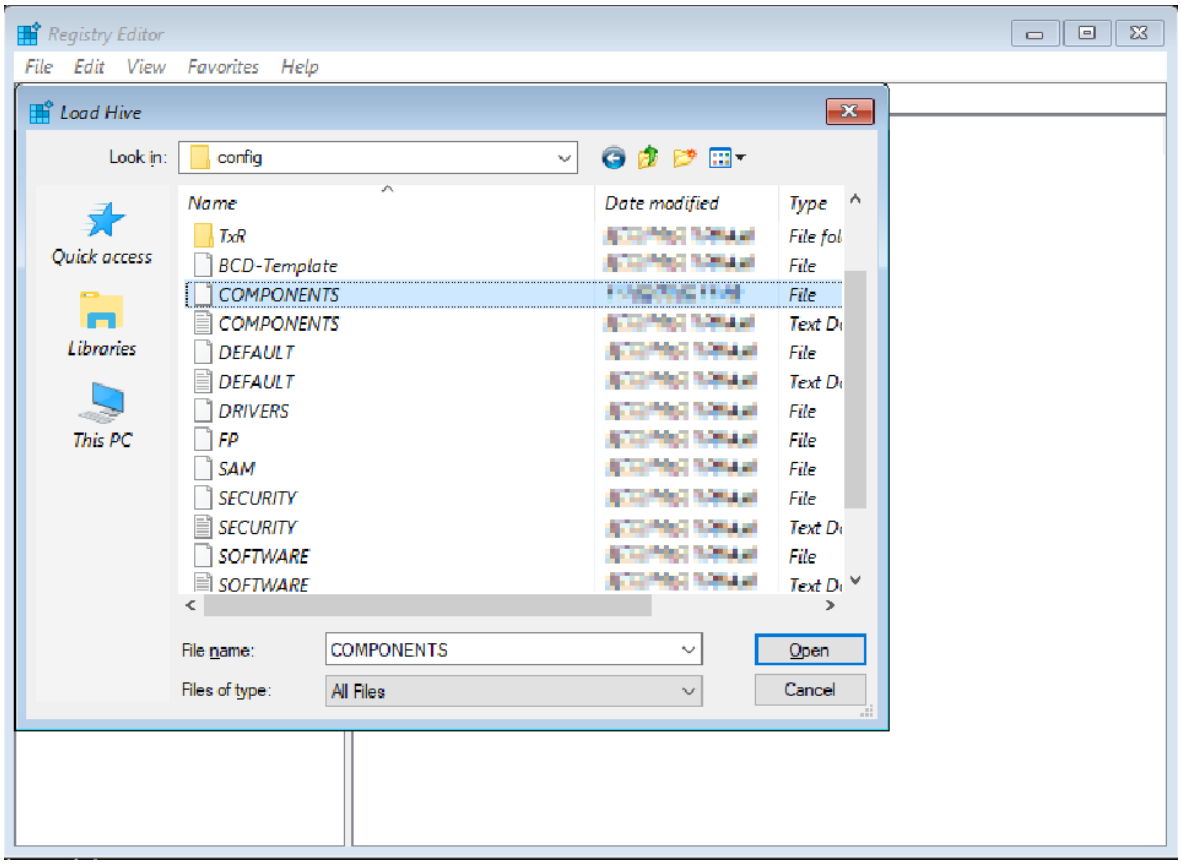

Reverting pending actions from the image...
The operation completed. Revert of pending actions will be attempted after the reboot.
The operation completed successfully.
```

2. Navigate to *OSdriveLetter:\Windows\WinSxS*, and then check whether the *pending.xml* file exists. If it does, rename it to *pending.xml.old*.

3. To revert the registry changes, type *regedit* at the command prompt to open **Registry Editor**.

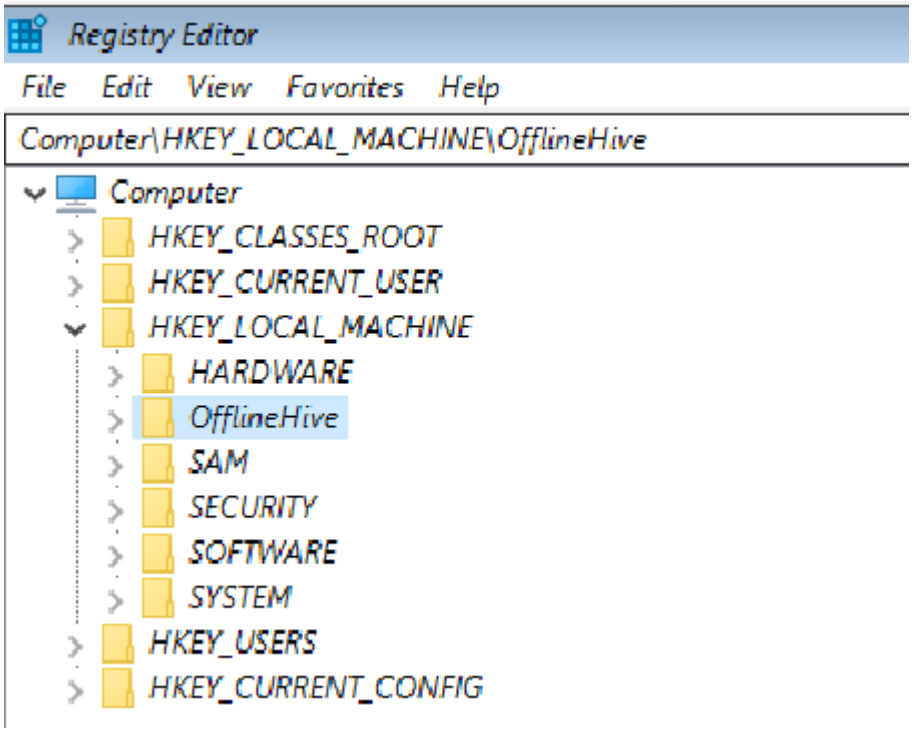
4. Select **HKEY_LOCAL_MACHINE**, and then go to **File** > **Load Hive**.

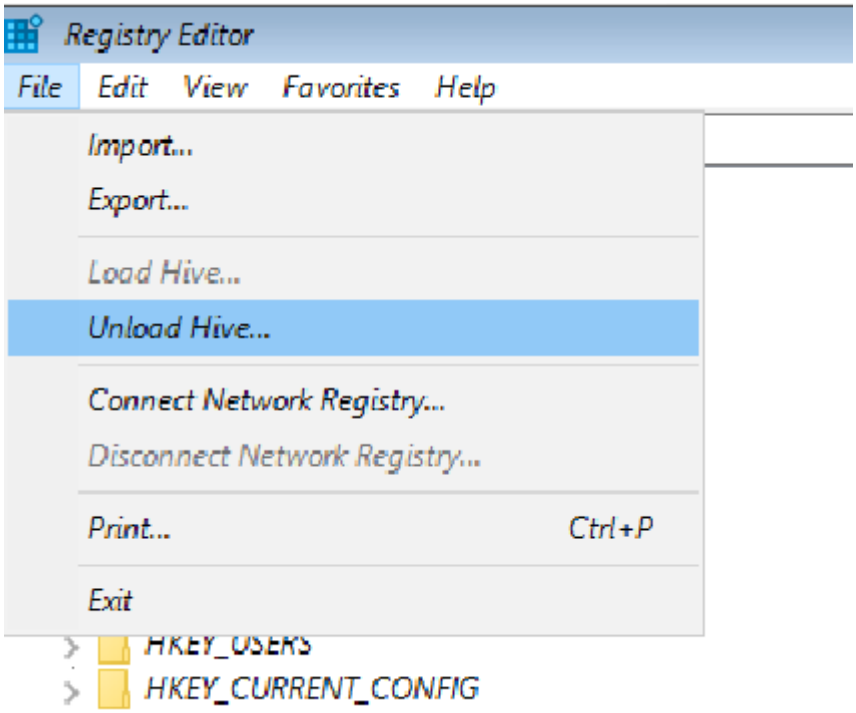
5. Navigate to *OSdriveLetter:\Windows\System32\config*, select the file that's named *COMPONENT* (with no extension), and then select **Open**. When you're prompted, enter the name *OfflineComponentHive* for the new hive.



6. Expand `HKEY_LOCAL_MACHINE\OfflineComponentHive`, and check whether the **PendingXmlIdentifier** key exists. Create a backup of the **OfflineComponentHive** key, and then delete the **PendingXmlIdentifier** key.

7. Unload the hive. To do this unloading, highlight **OfflineComponentHive**, and then select **File** > **Unload hive**.





8. Select **HKEY_LOCAL_MACHINE**, go to **File** > **Load Hive**, navigate to *OSdriveLetter:\Windows\System32\config*, select the file that's named **SYSTEM** (with no extension), and then select **Open**. When you're prompted, enter the name **OfflineSystemHive** for the new hive.

9. Expand **HKEY_LOCAL_MACHINE\OfflineSystemHive**, and then select the **Select** key. Check the data for the **Default** value.

10. If the data in `HKEY_LOCAL_MACHINE\OfflineSystemHive\Select\Default` is **1**, expand `HKEY_LOCAL_MACHINE\OfflineHive\ControlSet001`. If it's **2**, expand `HKEY_LOCAL_MACHINE\OfflineHive\ControlSet002`, and so on.

11. Expand `Control\Session Manager`. Check whether the **PendingFileRenameOperations** key exists. If it does, back up the **SessionManager** key, and then delete the **PendingFileRenameOperations** key.

Verifying boot critical drivers and services

Check services

1. Follow steps 1-10 in the "Troubleshooting if this issue occurs after a Windows Update installation" section. (Step 11 doesn't apply to this procedure.)
2. Expand **Services**.
3. Make sure that the following registry keys exist under **Services**:

   - ACPI
   - DISK
   - VOLMGR
   - PARTMGR
   - VOLSNAP
   - VOLUME

   If these keys exist, check each one to make sure that it has a value that's named **Start**, and that it's set to **0**. If it's not, set the value to **0**.

   If any of these keys don't exist, you can try to replace the current registry hive by using the hive from **RegBack**. To do this step, run the following commands:

   Console

   ```
   cd OSdrive:\Windows\System32\config
   ren SYSTEM SYSTEM.old
   copy OSdrive:\Windows\System32\config\RegBack\SYSTEM
   OSdrive:\Windows\System32\config\
   ```

Check upper and lower filter drivers

Check whether there are any non-Microsoft upper and lower filter drivers on the computer and that they don't exist on another, similar working computer. If they do exist, remove the upper and lower filter drivers:

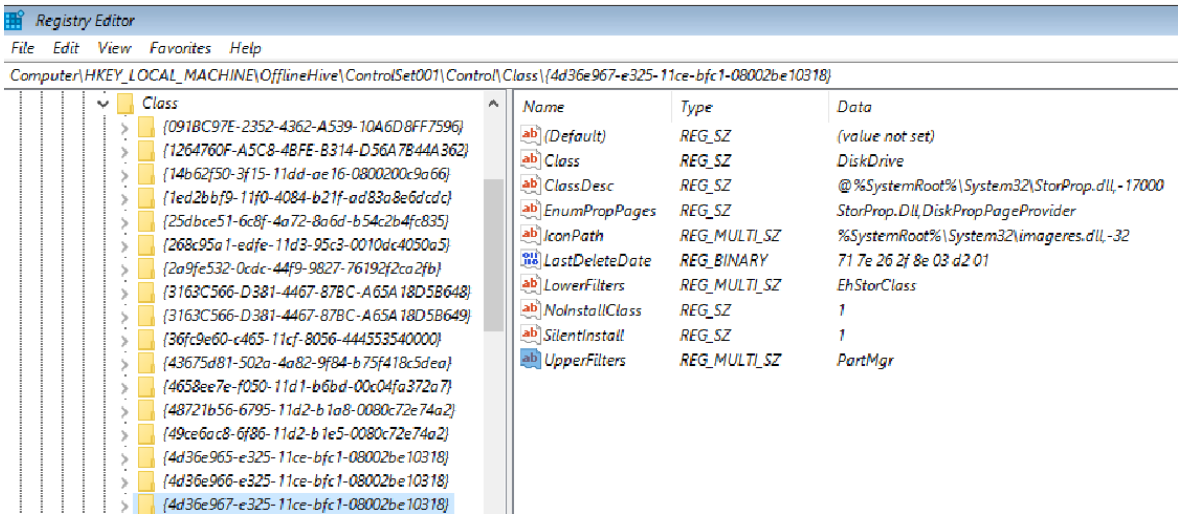
1. Expand `HKEY_LOCAL_MACHINE\OfflineHive\ControlSet001\Control`.

2. Look for any **UpperFilters** or **LowerFilters** entries.

> ⓘ **Note**
>
> These filters are mainly related to storage. After you expand the **Control** key in the registry, you can search for **UpperFilters** and **LowerFilters**.

You might find these filter drivers in some of the following registry entries. These entries are under **ControlSet** and are designated as **Default**:

- `\Control\Class\{4D36E96A-E325-11CE-BFC1-08002BE10318}`
- `\Control\Class\{4D36E967-E325-11CE-BFC1-08002BE10318}`
- `\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}`
- `\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}`



If an **UpperFilters** or **LowerFilters** entry is non-standard (for example, it's not a Windows default filter driver, such as PartMgr), remove the entry. To remove it, double-click it in the right pane, and then delete only that value.

> ⓘ **Note**
>
> There could be multiple entries.

These entries might affect us because there might be an entry in the **Services** branch that has a START type set to 0 or 1, which means that it's loaded at the Boot or Automatic part of the boot process. Also, either the file that's referred to is missing or corrupted, or it might be named differently than what's listed in the entry.

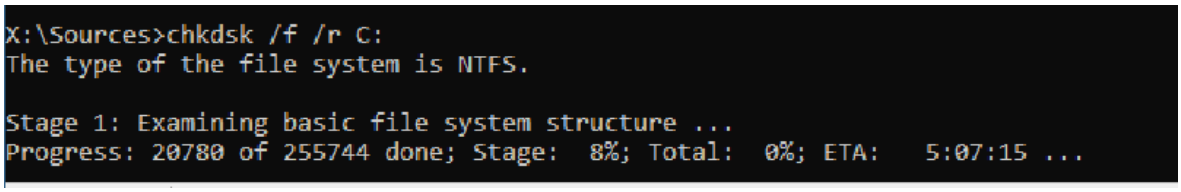
> ⓘ **Note**
>
> If there's a service that's set to **0** or **1** that corresponds to an **UpperFilters** or **LowerFilters** entry, setting the service to disabled in the **Services** registry (as discussed in steps 2 and 3 of the Check services section) without removing the **Filter Driver** entry causes the computer to crash and generate a 0x7b Stop error.

Running SFC and Chkdsk

If the computer still doesn't start, you can try to run a `chkdisk` process on the system drive, and then also run System File Checker. Do these steps by running the following commands at a WinRE command prompt:

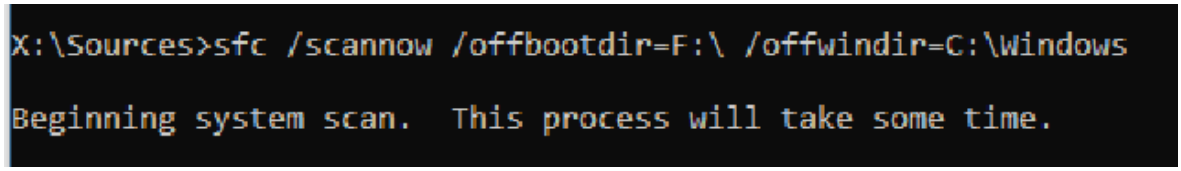
- Console

```
chkdsk /f /r OsDrive:
```



- Console

```
sfc /scannow /offbootdir=OsDrive:\ /offwindir=OsDrive:\Windows
```



Advanced troubleshooting for stop or blue screen errors

Article • 09/02/2022 • 19 minutes to read

Try our Virtual Agent - It can help you quickly identify and fix common Windows boot issues

> **Note**
>
> If you're not a support agent or IT professional, you'll find more helpful information about stop error ("blue screen") messages in **Troubleshoot blue screen errors**.

Applies to: Windows 10

What causes stop errors?

A stop error is displayed as a blue screen that contains the name of the faulty driver, such as any of the following example drivers:

- *atikmpag.sys*
- *igdkmd64.sys*
- *nvlddmkm.sys*

There's no simple explanation for the cause of stop errors (also known as blue screen errors or bug check errors). Many different factors can be involved. However, various studies indicate that stop errors usually aren't caused by Microsoft Windows components. Instead, these errors are related to malfunctioning hardware drivers or drivers that are installed by third-party software. These drivers include video cards, wireless network cards, security programs, and so on.

Our analysis of the root causes of crashes indicates that:

- 70% are caused by third-party driver code.
- 10% are caused by hardware issues.
- 5% are caused by Microsoft code.
- 15% have unknown causes, because the memory is too corrupted to analyze.

> **Note**

The root cause of stop errors is never a user-mode process. While a user-mode process (such as Notepad or Slack) may trigger a stop error, it is merely exposing the underlying bug which is always in a driver, hardware, or the OS.

General troubleshooting steps

To troubleshoot stop error messages, follow these general steps:

1. Review the stop error code that you find in the event logs. Search online for the specific stop error codes to see whether there are any known issues, resolutions, or workarounds for the problem.

2. Make sure that you install the latest Windows updates, cumulative updates, and rollup updates. To verify the update status, refer to the appropriate update history for your system. For example:

   - Windows 10, version 21H2
   - Windows 10, version 21H1
   - Windows 10, version 20H2

3. Make sure that the BIOS and firmware are up-to-date.

4. Run any relevant hardware and memory tests.

5. Run Microsoft Safety Scanner or any other virus detection program that includes checks of the MBR for infections.

6. Make sure that there's sufficient free space on the hard disk. The exact requirement varies, but we recommend 10-15 percent free disk space.

7. Contact the respective hardware or software vendor to update the drivers and applications in the following scenarios:

   - The error message indicates that a specific driver is causing the problem.
   - You're seeing an indication of a service that is starting or stopping before the crash occurred. In this situation, determine whether the service behavior is consistent across all instances of the crash.
   - You have made any software or hardware changes.

   > **Note**
   >
   > If there are no updates available from a specific manufacturer, we recommend that you disable the related service.

For more information, see **How to perform a clean boot in Windows**.

You can disable a driver by following the steps in **How to temporarily deactivate the kernel mode filter driver in Windows**.

You may also want to consider the option of rolling back changes or reverting to the last-known working state. For more information, see **Roll back a device driver to a previous version**.

Memory dump collection

To configure the system for memory dump files, follow these steps:

1. Select the Taskbar search box, type *Advanced system settings*, and then press **Enter**.
2. On the **Advanced** tab on the **System Properties** box, select the **Settings** button that appears in the section **Startup and Recovery**.
3. In the new window, select the drop-down below the option **Write debugging information**.
4. Choose **Automatic memory dump**.
5. Select **OK**.
6. Restart the computer for the setting to take effect.
7. If the server is virtualized, disable auto reboot after the memory dump file is created. This disablement lets you take a snapshot of the server in-state and also if the problem recurs.

The memory dump file is saved at the following locations:

Dump file type	Location
(none)	*%SystemRoot%\MEMORY.DMP* (inactive, or grayed out)
Small memory dump file (256 kb)	*%SystemRoot%\Minidump*
Kernel memory dump file	*%SystemRoot%\MEMORY.DMP*
Complete memory dump file	*%SystemRoot%\MEMORY.DMP*
Automatic memory dump file	*%SystemRoot%\MEMORY.DMP*
Active memory dump file	*%SystemRoot%\MEMORY.DMP*

You can use the Microsoft Crash Dump File Checker (DumpChk) tool to verify that the memory dump files aren't corrupted or invalid. For more information, see the following video:
https://www.youtube-nocookie.com/embed/xN7tOfgNKag

For more information on how to use *Dumpchk.exe* to check your dump files, see the following articles:

- Using DumpChk
- Download DumpChk

Pagefile settings

For more information on pagefile settings, see the following articles:

- Introduction to page files
- How to determine the appropriate page file size for 64-bit versions of Windows
- Generate a kernel or complete crash dump

Memory dump analysis

Finding the root cause of the crash may not be easy. Hardware problems are especially difficult to diagnose because they may cause erratic and unpredictable behavior that can manifest itself in various symptoms.

When a stop error occurs, you should first isolate the problematic components, and then try to cause them to trigger the stop error again. If you can replicate the problem, you can usually determine the cause.

You can use the tools such as Windows Software Development Kit (SDK) and symbols to diagnose dump logs. The next section discusses how to use this tool.

Advanced troubleshooting steps

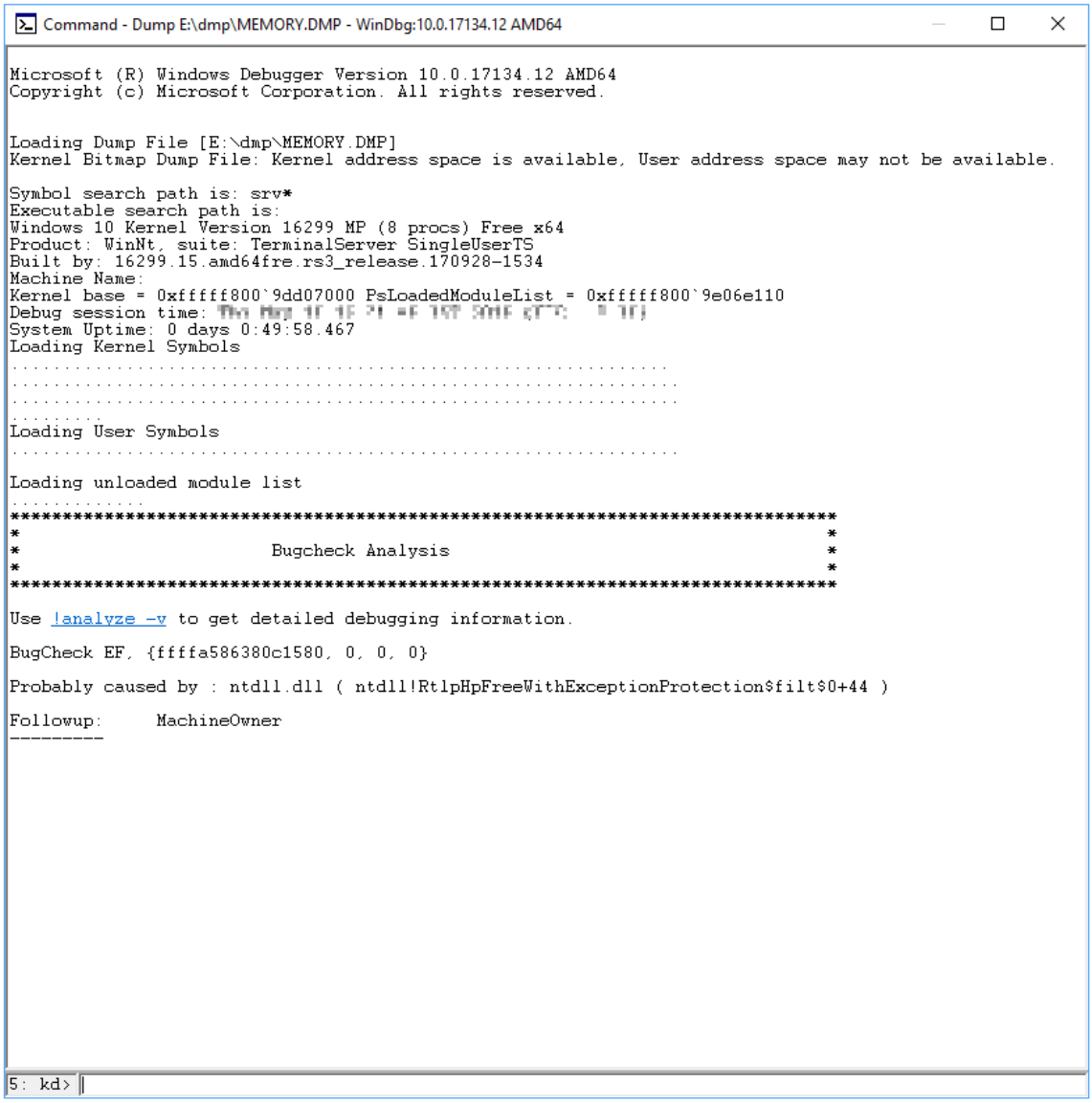
> **Note**
>
> Advanced troubleshooting of crash dumps can be very challenging if you aren't experienced with programming and internal Windows mechanisms. We have attempted to provide a brief insight here into some of the techniques used, including some examples. However, to really be effective at troubleshooting a crash dump, you should spend time becoming familiar with advanced debugging techniques. For a video overview, **Debugging kernel mode crashes and hangs**. Also see the advanced references listed below.

Advanced debugging references

- Advanced Windows Debugging, first edition book
- Debugging Tools for Windows (WinDbg, KD, CDB, NTSD)

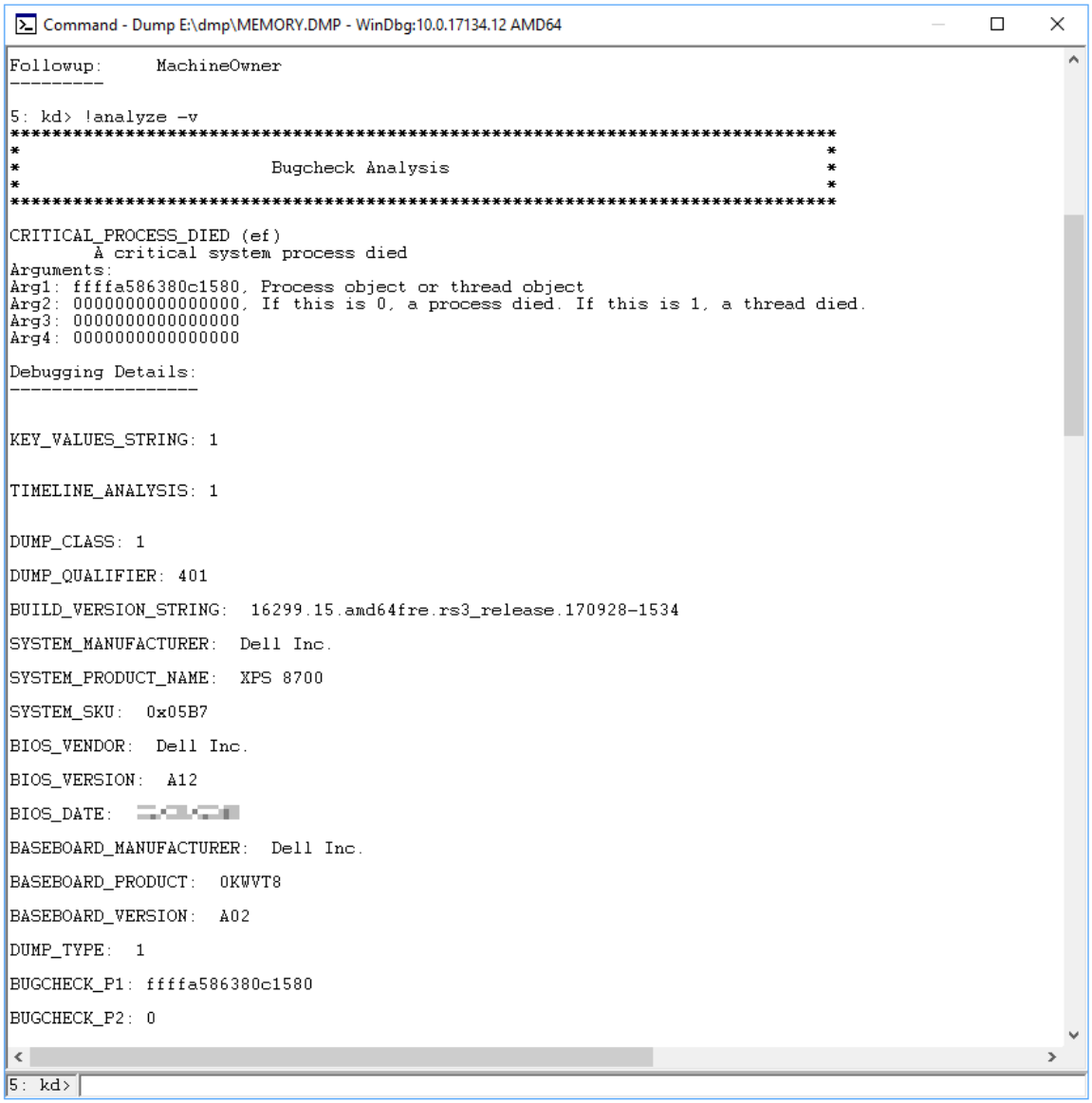
Debugging steps

1. Verify that the computer is set up to generate a complete memory dump file when a crash occurs. For more information, see Method 1: Memory dump.
2. Locate the *memory.dmp* file in your Windows directory on the computer that is crashing, and copy that file to another computer.
3. On the other computer, download the Windows 10 SDK.
4. Start the install and choose **Debugging Tools for Windows**. The WinDbg tool is installed.
5. Go to the **File** menu and select **Symbol File Path** to open the WinDbg tool and set the symbol path.
   a. If the computer is connected to the internet, enter the Microsoft public symbol server: `https://msdl.microsoft.com/download/symbols` and select **OK**. This method is recommended.
   b. If the computer isn't connected to the internet, specify a local symbol path.
6. Select **Open Crash Dump**, and then open the *memory.dmp* file that you copied.



7. Under **Bugcheck Analysis**, select **`!analyze -v`**. The command `!analyze -v` is entered in the prompt at the bottom of the page.

8. A detailed bug check analysis appears.



9. Scroll down to the **STACK_TEXT** section. There will be rows of numbers with each row followed by a colon and some text. That text should tell you what DLL is causing the crash. If applicable, it also says what service is crashing the DLL.

10. For more information about how to interpret the STACK_TEXT output, see Using the !analyze Extension.

There are many possible causes of a bug check and each case is unique. In the example provided above, the important lines that can be identified from the STACK_TEXT are 20, 21, and 22:

> **Note**
>
> HEX data is removed here and lines are numbered for clarity.

Output

```
1  : nt!KeBugCheckEx
2  : nt!PspCatchCriticalBreak+0xff
3  : nt!PspTerminateAllThreads+0x1134cf
4  : nt!PspTerminateProcess+0xe0
5  : nt!NtTerminateProcess+0xa9
6  : nt!KiSystemServiceCopyEnd+0x13
7  : nt!KiServiceLinkage
8  : nt!KiDispatchException+0x1107fe
9  : nt!KiFastFailDispatch+0xe4
10 : nt!KiRaiseSecurityCheckFailure+0x3d3
11 : ntdll!RtlpHpFreeWithExceptionProtection$filt$0+0x44
12 : ntdll!_C_specific_handler+0x96
13 : ntdll!RtlpExecuteHandlerForException+0xd
14 : ntdll!RtlDispatchException+0x358
15 : ntdll!KiUserExceptionDispatch+0x2e
16 : ntdll!RtlpHpVsContextFree+0x11e
17 : ntdll!RtlpHpFreeHeap+0x48c
18 : ntdll!RtlpHpFreeWithExceptionProtection+0xda
19 : ntdll!RtlFreeHeap+0x24a
20 : FWPolicyIOMgr!FwBinariesFree+0xa7c2
21 : mpssvc!FwMoneisDiagEdpPolicyUpdate+0x1584f
22 : mpssvc!FwEdpMonUpdate+0x6c
23 : ntdll!RtlpWnfWalkUserSubscriptionList+0x29b
24 : ntdll!RtlpWnfProcessCurrentDescriptor+0x105
25 : ntdll!RtlpWnfNotificationThread+0x80
26 : ntdll!TppExecuteWaitCallback+0xe1
27 : ntdll!TppWorkerThread+0x8d0
28 : KERNEL32!BaseThreadInitThunk+0x14
29 : ntdll!RtlUserThreadStart+0x21
```

This issue is because of the mpssvc service, which is a component of the Windows Firewall. The problem was repaired by disabling the firewall temporarily and then resetting firewall policies.

For more examples, see Debugging examples.

Video resources

The following videos illustrate various troubleshooting techniques for analyzing dump files.

- Analyze dump file
- Installing debugging tool for Windows (x64 and x86)
- Debugging kernel mode crash memory dumps
- Special pool

Advanced troubleshooting using Driver Verifier

We estimate that about 75 percent of all stop errors are caused by faulty drivers. The Driver Verifier tool provides several methods to help you troubleshoot. These include running drivers in an isolated memory pool (without sharing memory with other components), generating extreme memory pressure, and validating parameters. If the tool encounters errors in the execution of driver code, it proactively creates an exception. It can then further examine that part of the code.

> ⚠ **Warning**
>
> Driver Verifier consumes lots of CPU and can slow down the computer significantly. You may also experience additional crashes. Verifier disables faulty drivers after a stop error occurs, and continues to do this until you can successfully restart the system and access the desktop. You can also expect to see several dump files created.
>
> Don't try to verify all the drivers at one time. This action can degrade performance and make the system unusable. It also limits the effectiveness of the tool.

Use the following guidelines when you use Driver Verifier:

- Test any "suspicious" drivers. For example, drivers that were recently updated or that are known to be problematic.
- If you continue to experience non-analyzable crashes, try enabling verification on all third-party and unsigned drivers.
- Enable concurrent verification on groups of 10-20 drivers.
- Additionally, if the computer can't boot into the desktop because of Driver Verifier, you can disable the tool by starting in Safe mode. This solution is because the tool can't run in Safe mode.

For more information, see Driver Verifier.

Common Windows stop errors

This section doesn't contain a list of all error codes, but since many error codes have the same potential resolutions, your best bet is to follow the steps below to troubleshoot your error.

The following sections list general troubleshooting procedures for common stop error codes.

VIDEO_ENGINE_TIMEOUT_DETECTED or VIDEO_TDR_TIMEOUT_DETECTED

Stop error code 0x00000141, or 0x00000117

Contact the vendor of the listed display driver to get an appropriate update for that driver.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

Stop error code 0x0000000D1

Apply the latest updates for the driver by applying the latest cumulative updates for the system through the Microsoft Update Catalog website. Update an outdated network driver. Virtualized VMware systems often run "Intel(R) PRO/1000 MT Network Connection" (e1g6032e.sys). You can download this driver from the Intel Download Drivers & Software website. Contact the hardware vendor to update the network driver for a resolution. For VMware systems, use the VMware integrated network driver instead of Intel's e1g6032e.sys. For example, use VMware types VMXNET, VMXNET2, or VMXNET3.

PAGE_FAULT_IN_NONPAGED_AREA

Stop error code 0x000000050

If a driver is identified in the stop error message, contact the manufacturer for an update. If no updates are available, disable the driver, and monitor the system for stability. Run `chkdsk /f /r` to detect and repair disk errors. Restart the system before the disk scan begins on a system partition. Contact the manufacturer for any diagnostic tools that they may provide for the hard disk subsystem. Try to reinstall any application or service that was recently installed or updated. It's possible that the crash was triggered while the system was starting applications and reading the registry for preference settings. Reinstalling the application can fix corrupted registry keys. If the problem persists, and you have run a recent system state backup, try to restore the registry hives from the backup.

SYSTEM_SERVICE_EXCEPTION

Stop error code c000021a {Fatal System Error} The Windows SubSystem system process terminated unexpectedly with a status of 0xc0000005. The system has been shut down.

Use the System File Checker tool to repair missing or corrupted system files. The System File Checker lets users scan for corruptions in Windows system files and restore corrupted files. For more information, see Use the System File Checker tool.

NTFS_FILE_SYSTEM

Stop error code 0x000000024

This stop error is commonly caused by corruption in the NTFS file system or bad blocks (sectors) on the hard disk. Corrupted drivers for hard disks (SATA or IDE) can also adversely affect the system's ability to read and write to disk. Run any hardware diagnostics that are provided by the manufacturer of the storage subsystem. Use the scan disk tool to verify that there are no file system errors. To do this step, right-click the drive that you want to scan, select Properties, select Tools, and then select the Check now button. Update the NTFS file system driver (Ntfs.sys). Apply the latest cumulative updates for the current operating system that's experiencing the problem.

KMODE_EXCEPTION_NOT_HANDLED

Stop error code 0x0000001E

If a driver is identified in the stop error message, disable or remove that driver. Disable or remove any drivers or services that were recently added.

If the error occurs during the startup sequence, and the system partition is formatted by using the NTFS file system, you might be able to use safe mode to disable the driver in Device Manager. To disable the driver, follow these steps:

1. Go to **Settings** > **Update & security** > **Recovery**.
2. Under **Advanced startup**, select **Restart now**.
3. After your PC restarts to the **Choose an option** screen, select **Troubleshoot** > **Advanced options** > **Startup Settings** > **Restart**.
4. After the computer restarts, you'll see a list of options. Press 4 or F4 to start the computer in safe mode. If you intend to use the internet while in safe mode, press 5 or F5 for the **Safe Mode with Networking** option.

DPC_WATCHDOG_VIOLATION

Stop error code 0x00000133

This stop error code is caused by a faulty driver that doesn't complete its work within the allotted time frame in certain conditions. To help mitigate this error, collect the

memory dump file from the system, and then use the Windows Debugger to find the faulty driver. If a driver is identified in the stop error message, disable the driver to isolate the problem. Check with the manufacturer for driver updates. Check the system log in Event Viewer for other error messages that might help identify the device or driver that's causing stop error 0x133. Verify that any new hardware that's installed is compatible with the installed version of Windows. For example, you can get information about required hardware at Windows 10 Specifications. If Windows Debugger is installed, and you have access to public symbols, you can load the *c:\windows\memory.dmp* file into the debugger. Then refer to Determining the source of Bug Check 0x133 (DPC_WATCHDOG_VIOLATION) errors on Windows Server 2012 to find the problematic driver from the memory dump.

USER_MODE_HEALTH_MONITOR

Stop error code 0x0000009E

This stop error indicates that a user-mode health check failed in a way that prevents graceful shutdown. Windows restores critical services by restarting or enabling application failover to other servers. The Clustering Service incorporates a detection mechanism that may detect unresponsiveness in user-mode components.

This stop error usually occurs in a clustered environment, and the indicated faulty driver is RHS.exe. Check the event logs for any storage failures to identify the failing process. Try to update the component or process that's indicated in the event logs. You should see the following event recorded:

- Event ID: 4870
- Source: Microsoft-Windows-FailoverClustering
- Description: User mode health monitoring has detected that the system isn't being responsive. The Failover cluster virtual adapter has lost contact with the Cluster Server process with a process ID '%1', for '%2' seconds. Recovery action is taken. Review the Cluster logs to identify the process and investigate which items might cause the process to hang.

For more information, see "0x0000009E" Stop error on cluster nodes in a Windows Server-based multi-node failover cluster environment Also, see the following Microsoft video What to do if a 9E occurs.

Debugging examples

Example 1

This bug check is caused by a driver hang during upgrade, resulting in a bug check D1 in *NDIS.sys*, which is a Microsoft driver. The IMAGE_NAME tells you the faulting driver, but since this driver is s Microsoft driver, it can't be replaced or removed. The resolution method is to disable the network device in device manager and try the upgrade again.

Console

```
2: kd> !analyze -v
*******************************************************************************
***
*
*
*                        Bugcheck Analysis
*
*
*
*******************************************************************************
***

DRIVER_IRQL_NOT_LESS_OR_EQUAL (d1)
An attempt was made to access a pageable (or completely invalid) address at
an
interrupt request level (IRQL) that is too high.  This is usually
caused by drivers using improper addresses.
If kernel debugger is available get stack backtrace.
Arguments:
Arg1: 000000000011092a, memory referenced
Arg2: 0000000000000002, IRQL
Arg3: 0000000000000001, value 0 = read operation, 1 = write operation
Arg4: fffff807aa74f4c4, address which referenced memory
Debugging Details:
------------------

KEY_VALUES_STRING: 1
STACKHASH_ANALYSIS: 1
TIMELINE_ANALYSIS: 1
DUMP_CLASS: 1
DUMP_QUALIFIER: 400
SIMULTANEOUS_TELSVC_INSTANCES:  0
SIMULTANEOUS_TELWP_INSTANCES:  0
BUILD_VERSION_STRING:  16299.15.amd64fre.rs3_release.170928-1534
SYSTEM_MANUFACTURER:  Alienware
SYSTEM_PRODUCT_NAME:  Alienware 15 R2
SYSTEM_SKU:  Alienware 15 R2
SYSTEM_VERSION:  1.2.8
BIOS_VENDOR:  Alienware
BIOS_VERSION:  1.2.8
BIOS_DATE:  01/29/2016
BASEBOARD_MANUFACTURER:  Alienware
BASEBOARD_PRODUCT:  Alienware 15 R2
BASEBOARD_VERSION:  A00
DUMP_TYPE:  2
BUGCHECK_P1: 11092a
```

```
BUGCHECK_P2: 2
BUGCHECK_P3: 1
BUGCHECK_P4: fffff807aa74f4c4
WRITE_ADDRESS: fffff80060602380: Unable to get MiVisibleState
Unable to get NonPagedPoolStart
Unable to get NonPagedPoolEnd
Unable to get PagedPoolStart
Unable to get PagedPoolEnd
000000000011092a
CURRENT_IRQL:  2
FAULTING_IP:
NDIS!NdisQueueIoWorkItem+4 [minio\ndis\sys\miniport.c @ 9708]
fffff807`aa74f4c4 48895120        mov     qword ptr [rcx+20h],rdx
CPU_COUNT: 8
CPU_MHZ: a20
CPU_VENDOR:  GenuineIntel
CPU_FAMILY: 6
CPU_MODEL: 5e
CPU_STEPPING: 3
CPU_MICROCODE: 6,5e,3,0 (F,M,S,R)  SIG: BA'00000000 (cache) BA'00000000
(init)
BLACKBOXPNP: 1 (!blackboxpnp)
DEFAULT_BUCKET_ID:  WIN8_DRIVER_FAULT
BUGCHECK_STR:  AV
PROCESS_NAME:  System
ANALYSIS_SESSION_HOST:  SHENDRIX-DEV0
ANALYSIS_SESSION_TIME:  01-17-2019 11:06:05.0653
ANALYSIS_VERSION: 10.0.18248.1001 amd64fre
TRAP_FRAME:  ffffa884c0c3f6b0 -- (.trap 0xffffa884c0c3f6b0)
NOTE: The trap frame doesn't contain all registers.
Some register values may be zeroed or incorrect.
rax=fffff807ad018bf0 rbx=0000000000000000 rcx=000000000011090a
rdx=fffff807ad018c10 rsi=0000000000000000 rdi=0000000000000000
rip=fffff807aa74f4c4 rsp=ffffa884c0c3f840 rbp=000000002408fd00
r8=ffffb30e0e99ea30  r9=0000000001d371c1 r10=0000000020000080
r11=0000000000000000 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iopl=0         nv up ei ng nz na pe nc
NDIS!NdisQueueIoWorkItem+0x4:
fffff807`aa74f4c4 48895120        mov     qword ptr [rcx+20h],rdx
ds:00000000`0011092a=????????????????
Resetting default scope

LAST_CONTROL_TRANSFER:  from fffff800603799e9 to fffff8006036e0e0

STACK_TEXT:
ffffa884`c0c3f568 fffff800`603799e9 : 00000000`0000000a 00000000`0011092a
00000000`00000002 00000000`00000001 : nt!KeBugCheckEx
[minkernel\ntos\ke\amd64\procstat.asm @ 134]
ffffa884`c0c3f570 fffff800`60377d7d : fffff78a`4000a150 ffffb30e`03fba001
ffff8180`f0b5d180 00000000`000000ff : nt!KiBugCheckDispatch+0x69
[minkernel\ntos\ke\amd64\trap.asm @ 2998]
ffffa884`c0c3f6b0 fffff807`aa74f4c4 : 00000000`00000002 ffff8180`f0754180
00000000`00269fb1 ffff8180`f0754180 : nt!KiPageFault+0x23d
[minkernel\ntos\ke\amd64\trap.asm @ 1248]
```

```
ffffa884`c0c3f840 fffff800`60256b63 : ffffb30e`0e18f710 ffff8180`f0754180
ffffa884`c0c3fa18 00000000`00000002 : NDIS!NdisQueueIoWorkItem+0x4
[minio\ndis\sys\miniport.c @ 9708]
ffffa884`c0c3f870 fffff800`60257bfd : 00000000`00000008 00000000`00000000
00000000`00269fb1 ffff8180`f0754180 : nt!KiProcessExpiredTimerList+0x153
[minkernel\ntos\ke\dpcsup.c @ 2078]
ffffa884`c0c3f960 fffff800`6037123a : 00000000`00000000 ffff8180`f0754180
00000000`00000000 ffff8180`f0760cc0 : nt!KiRetireDpcList+0x43d
[minkernel\ntos\ke\dpcsup.c @ 1512]
ffffa884`c0c3fb60 00000000`00000000 : ffffa884`c0c40000 ffffa884`c0c39000
00000000`00000000 00000000`00000000 : nt!KiIdleLoop+0x5a
[minkernel\ntos\ke\amd64\idle.asm @ 166]

RETRACER_ANALYSIS_TAG_STATUS:  Failed in getting KPCR for core 2
THREAD_SHA1_HASH_MOD_FUNC:  5b59a784f22d4b5cbd5a8452fe39914b8fd7961d
THREAD_SHA1_HASH_MOD_FUNC_OFFSET:  5643383f9cae3ca39073f7721b53f0c633bfb948
THREAD_SHA1_HASH_MOD:  20edda059578820e64b723e466deea47f59bd675
FOLLOWUP_IP:
NDIS!NdisQueueIoWorkItem+4 [minio\ndis\sys\miniport.c @ 9708]
fffff807`aa74f4c4 48895120        mov     qword ptr [rcx+20h],rdx
FAULT_INSTR_CODE:  20518948
FAULTING_SOURCE_LINE:  minio\ndis\sys\miniport.c
FAULTING_SOURCE_FILE:  minio\ndis\sys\miniport.c
FAULTING_SOURCE_LINE_NUMBER:  9708
FAULTING_SOURCE_CODE:
  9704:     _In_ _Points_to_data_      PVOID
WorkItemContext
  9705:     )
  9706: {
  9707:
> 9708:     ((PNDIS_IO_WORK_ITEM)NdisIoWorkItemHandle)->Routine = Routine;
  9709:     ((PNDIS_IO_WORK_ITEM)NdisIoWorkItemHandle)->WorkItemContext =
WorkItemContext;
  9710:
  9711:     IoQueueWorkItem(((PNDIS_IO_WORK_ITEM)NdisIoWorkItemHandle)-
>IoWorkItem,
  9712:                     ndisDispatchIoWorkItem,
  9713:                     CriticalWorkQueue,

SYMBOL_STACK_INDEX:  3
SYMBOL_NAME:  NDIS!NdisQueueIoWorkItem+4
FOLLOWUP_NAME:  ndiscore
MODULE_NAME: NDIS
IMAGE_NAME:  NDIS.SYS
DEBUG_FLR_IMAGE_TIMESTAMP:  0
IMAGE_VERSION:  10.0.16299.99
DXGANALYZE_ANALYSIS_TAG_PORT_GLOBAL_INFO_STR:  Hybrid_FALSE
DXGANALYZE_ANALYSIS_TAG_ADAPTER_INFO_STR:
GPU0_VenId0x1414_DevId0x8d_WDDM1.3_Active;
STACK_COMMAND:  .thread ; .cxr ; kb
BUCKET_ID_FUNC_OFFSET:  4
FAILURE_BUCKET_ID:  AV_NDIS!NdisQueueIoWorkItem
BUCKET_ID:  AV_NDIS!NdisQueueIoWorkItem
PRIMARY_PROBLEM_CLASS:  AV_NDIS!NdisQueueIoWorkItem
TARGET_TIME:  2017-12-10T14:16:08.000Z
```

```
OSBUILD:  16299
OSSERVICEPACK:  98
SERVICEPACK_NUMBER: 0
OS_REVISION: 0
SUITE_MASK:  784
PRODUCT_TYPE:  1
OSPLATFORM_TYPE:  x64
OSNAME:  Windows 10
OSEDITION:  Windows 10 WinNt TerminalServer SingleUserTS Personal
OS_LOCALE:
USER_LCID:  0
OSBUILD_TIMESTAMP:  2017-11-26 03:49:20
BUILDDATESTAMP_STR:  170928-1534
BUILDLAB_STR:  rs3_release
BUILDOSVER_STR:  10.0.16299.15.amd64fre.rs3_release.170928-1534
ANALYSIS_SESSION_ELAPSED_TIME:  8377
ANALYSIS_SOURCE:  KM
FAILURE_ID_HASH_STRING:  km:av_ndis!ndisqueueioworkitem
FAILURE_ID_HASH:  {10686423-afa1-4852-ad1b-9324ac44ac96}
FAILURE_ID_REPORT_LINK: https://go.microsoft.com/fwlink/?
LinkID=397724&FailureHash=10686423-afa1-4852-ad1b-9324ac44ac96
Followup:     ndiscore
---------
```

Example 2

In this example, a non-Microsoft driver caused page fault, so we don't have symbols for this driver. However, looking at IMAGE_NAME and or MODULE_NAME indicates it's *WwanUsbMP.sys* that caused the issue. Disconnecting the device and retrying the upgrade is a possible solution.

Console

```
1: kd> !analyze -v
*******************************************************************************
***
*
*
*                        Bugcheck Analysis
*
*
*
*******************************************************************************
***

PAGE_FAULT_IN_NONPAGED_AREA (50)
Invalid system memory was referenced.  This can't be protected by try-
except.
Typically the address is just plain bad or it is pointing at freed memory.
Arguments:
Arg1: 8ba10000, memory referenced.
```

```
Arg2: 00000000, value 0 = read operation, 1 = write operation.
Arg3: 82154573, If non-zero, the instruction address which referenced the
bad memory
                address.
Arg4: 00000000, (reserved)

Debugging Details:
------------------

*** WARNING: Unable to verify timestamp for WwanUsbMp.sys
*** ERROR: Module load completed but symbols could not be loaded for
WwanUsbMp.sys

KEY_VALUES_STRING: 1
STACKHASH_ANALYSIS: 1
TIMELINE_ANALYSIS: 1
DUMP_CLASS: 1
DUMP_QUALIFIER: 400
BUILD_VERSION_STRING:  16299.15.x86fre.rs3_release.170928-1534
MARKER_MODULE_NAME:  IBM_ibmpmdrv
SYSTEM_MANUFACTURER:  LENOVO
SYSTEM_PRODUCT_NAME:  20AWS07H00
SYSTEM_SKU:  LENOVO_MT_20AW_BU_Think_FM_ThinkPad T440p
SYSTEM_VERSION:  ThinkPad T440p
BIOS_VENDOR:  LENOVO
BIOS_VERSION:  GLET85WW (2.39 )
BIOS_DATE:  09/29/2016
BASEBOARD_MANUFACTURER:  LENOVO
BASEBOARD_PRODUCT:  20AWS07H00
BASEBOARD_VERSION:  Not Defined
DUMP_TYPE:  2
BUGCHECK_P1: ffffffff8ba10000
BUGCHECK_P2: 0
BUGCHECK_P3: ffffffff82154573
BUGCHECK_P4: 0
READ_ADDRESS: 822821d0: Unable to get MiVisibleState
8ba10000
FAULTING_IP:
nt!memcpy+33 [minkernel\crts\crtw32\string\i386\memcpy.asm @ 213
82154573 f3a5            rep movs dword ptr es:[edi],dword ptr [esi]
MM_INTERNAL_CODE:  0
CPU_COUNT: 4
CPU_MHZ: 95a
CPU_VENDOR:  GenuineIntel
CPU_FAMILY: 6
CPU_MODEL: 3c
CPU_STEPPING: 3
CPU_MICROCODE: 6,3c,3,0 (F,M,S,R)  SIG: 21'00000000 (cache) 21'00000000
(init)
BLACKBOXBSD: 1 (!blackboxbsd)
BLACKBOXPNP: 1 (!blackboxpnp)
DEFAULT_BUCKET_ID:  WIN8_DRIVER_FAULT
BUGCHECK_STR:  AV
PROCESS_NAME:  System
CURRENT_IRQL:  2
```

```
ANALYSIS_SESSION_HOST:  SHENDRIX-DEV0
ANALYSIS_SESSION_TIME:  01-17-2019 10:54:53.0780
ANALYSIS_VERSION: 10.0.18248.1001 amd64fre
TRAP_FRAME:  8ba0efa8 -- (.trap 0xffffffff8ba0efa8)
ErrCode = 00000000
eax=8ba1759e ebx=a2bfd314 ecx=00001d67 edx=00000002 esi=8ba10000
edi=a2bfe280
eip=82154573 esp=8ba0f01c ebp=8ba0f024 iopl=0         nv up ei pl nz ac pe
nc
cs=0008  ss=0010  ds=0023  es=0023  fs=0030  gs=0000
efl=00010216
nt!memcpy+0x33:
82154573 f3a5            rep movs dword ptr es:[edi],dword ptr [esi]
Resetting default scope
LOCK_ADDRESS:  8226c6e0 -- (!locks 8226c6e0)
Cannot get _ERESOURCE type
Resource @ nt!PiEngineLock (0x8226c6e0)    Available
1 total locks
PNP_TRIAGE_DATA:
                Lock address  : 0x8226c6e0
                Thread Count  : 0
                Thread address: 0x00000000
                Thread wait   : 0x0

LAST_CONTROL_TRANSFER:  from 82076708 to 821507e8

STACK_TEXT:
8ba0ede4 82076708 00000050 8ba10000 00000000 nt!KeBugCheckEx
[minkernel\ntos\ke\i386\procstat.asm @ 114]
8ba0ee40 8207771e 8ba0efa8 8ba10000 8ba0eea0 nt!MiSystemFault+0x13c8
[minkernel\ntos\mm\mmfault.c @ 4755]
8ba0ef08 821652ac 00000000 8ba10000 00000000 nt!MmAccessFault+0x83e
[minkernel\ntos\mm\mmfault.c @ 6868]
8ba0ef08 82154573 00000000 8ba10000 00000000 nt!_KiTrap0E+0xec
[minkernel\ntos\ke\i386\trap.asm @ 5153]
8ba0f024 86692866 a2bfd314 8ba0f094 0000850a nt!memcpy+0x33
[minkernel\crts\crtw32\string\i386\memcpy.asm @ 213]
8ba0f040 866961bc 8ba0f19c a2bfd0e8 00000000
NDIS!ndisMSetPowerManagementCapabilities+0x8a [minio\ndis\sys\miniport.c @
7969]
8ba0f060 866e1f66 866e1caf adfb9000 00000000
NDIS!ndisMSetGeneralAttributes+0x23d [minio\ndis\sys\miniport.c @ 8198]
8ba0f078 ac50c15f a2bfd0e8 0000009f 00000001
NDIS!NdisMSetMiniportAttributes+0x2b7 [minio\ndis\sys\miniport.c @ 7184]
WARNING: Stack unwind information not available. Following frames may be
wrong.
8ba0f270 ac526f96 adfb9000 a2bfd0e8 8269b9b0 WwanUsbMp+0x1c15f
8ba0f3cc 866e368a a2bfd0e8 00000000 8ba0f4c0 WwanUsbMp+0x36f96
8ba0f410 867004b0 a2bfd0e8 a2bfd0e8 a2be2a70 NDIS!ndisMInvokeInitialize+0x60
[minio\ndis\sys\miniport.c @ 13834]
8ba0f7ac 866dbc8e a2acf730 866b807c 00000000
NDIS!ndisMInitializeAdapter+0xa23 [minio\ndis\sys\miniport.c @ 601]
8ba0f7d8 866e687d a2bfd0e8 00000000 00000000 NDIS!ndisInitializeAdapter+0x4c
[minio\ndis\sys\initpnp.c @ 931]
8ba0f800 866e90bb adfb64d8 00000000 a2bfd0e8 NDIS!ndisPnPStartDevice+0x118
```

```
[minio\ndis\sys\configm.c @ 4235]
8ba0f820 866e8a58 adfb64d8 a2bfd0e8 00000000
NDIS!ndisStartDeviceSynchronous+0xbd [minio\ndis\sys\ndispnp.c @ 3096]
8ba0f838 866e81df adfb64d8 8ba0f85e 8ba0f85f NDIS!ndisPnPIrpStartDevice+0xb4
[minio\ndis\sys\ndispnp.c @ 1067]
8ba0f860 820a7e98 a2bfd030 adfb64d8 8ba0f910 NDIS!ndisPnPDispatch+0x108
[minio\ndis\sys\ndispnp.c @ 2429]
8ba0f878 8231f07e 8ba0f8ec adf5d4c8 872e2eb8 nt!IofCallDriver+0x48
[minkernel\ntos\io\iomgr\iosubs.c @ 3149]
8ba0f898 820b8569 820c92b8 872e2eb8 8ba0f910 nt!PnpAsynchronousCall+0x9e
[minkernel\ntos\io\pnpmgr\irp.c @ 3005]
8ba0f8cc 820c9a76 00000000 820c92b8 872e2eb8 nt!PnpSendIrp+0x67
[minkernel\ntos\io\pnpmgr\irp.h @ 286]
8ba0f914 8234577b 872e2eb8 adf638b0 adf638b0 nt!PnpStartDevice+0x60
[minkernel\ntos\io\pnpmgr\irp.c @ 3187]
8ba0f94c 82346cc7 872e2eb8 adf638b0 adf638b0 nt!PnpStartDeviceNode+0xc3
[minkernel\ntos\io\pnpmgr\start.c @ 1712]
8ba0f96c 82343c68 00000000 a2bdb3d8 adf638b0 nt!PipProcessStartPhase1+0x4d
[minkernel\ntos\io\pnpmgr\start.c @ 114]
8ba0fb5c 824db885 8ba0fb80 00000000 00000000 nt!PipProcessDevNodeTree+0x386
[minkernel\ntos\io\pnpmgr\enum.c @ 6129]
8ba0fb88 8219571b 85852520 8c601040 8226ba90 nt!PiRestartDevice+0x91
[minkernel\ntos\io\pnpmgr\enum.c @ 4743]
8ba0fbe8 820804af 00000000 00000000 8c601040
nt!PnpDeviceActionWorker+0xdb4b7 [minkernel\ntos\io\pnpmgr\action.c @ 674]
8ba0fc38 8211485c 85852520 421de295 00000000 nt!ExpWorkerThread+0xcf
[minkernel\ntos\ex\worker.c @ 4270]
8ba0fc70 82166785 820803e0 85852520 00000000 nt!PspSystemThreadStartup+0x4a
[minkernel\ntos\ps\psexec.c @ 7756]
8ba0fc88 82051e07 85943940 8ba0fcd8 82051bb9 nt!KiThreadStartup+0x15
[minkernel\ntos\ke\i386\threadbg.asm @ 82]
8ba0fc94 82051bb9 8b9cc600 8ba10000 8ba0d000
nt!KiProcessDeferredReadyList+0x17 [minkernel\ntos\ke\thredsup.c @ 5309]
8ba0fcd8 00000000 00000000 00000000 00000000 nt!KeSetPriorityThread+0x249
[minkernel\ntos\ke\thredobj.c @ 3881]


RETRACER_ANALYSIS_TAG_STATUS:  Failed in getting KPCR for core 1
THREAD_SHA1_HASH_MOD_FUNC:  e029276c66aea80ba36903e89947127118d31128
THREAD_SHA1_HASH_MOD_FUNC_OFFSET:  012389f065d31c8eedd6204846a560146a38099b
THREAD_SHA1_HASH_MOD:  44dc639eb162a28d47eaeeae4afe6f9eeccced3d
FOLLOWUP_IP:
WwanUsbMp+1c15f
ac50c15f 8bf0            mov     esi,eax
FAULT_INSTR_CODE:  f33bf08b
SYMBOL_STACK_INDEX:  8
SYMBOL_NAME:  WwanUsbMp+1c15f
FOLLOWUP_NAME:  MachineOwner
MODULE_NAME: WwanUsbMp
IMAGE_NAME:  WwanUsbMp.sys
DEBUG_FLR_IMAGE_TIMESTAMP:  5211bb0c
DXGANALYZE_ANALYSIS_TAG_PORT_GLOBAL_INFO_STR:  Hybrid_FALSE
DXGANALYZE_ANALYSIS_TAG_ADAPTER_INFO_STR:
GPU0_VenId0x1414_DevId0x8d_WDDM1.3_NotActive;GPU1_VenId0x8086_DevId0x416_WDD
M1.3_Active_Post;
```

```
STACK_COMMAND:  .thread ; .cxr ; kb
BUCKET_ID_FUNC_OFFSET:  1c15f
FAILURE_BUCKET_ID:  AV_R_INVALID_WwanUsbMp!unknown_function
BUCKET_ID:  AV_R_INVALID_WwanUsbMp!unknown_function
PRIMARY_PROBLEM_CLASS:  AV_R_INVALID_WwanUsbMp!unknown_function
TARGET_TIME:  2018-02-12T11:33:51.000Z
OSBUILD:  16299
OSSERVICEPACK:  15
SERVICEPACK_NUMBER: 0
OS_REVISION: 0
SUITE_MASK:  272
PRODUCT_TYPE:  1
OSPLATFORM_TYPE:  x86
OSNAME:  Windows 10
OSEDITION:  Windows 10 WinNt TerminalServer SingleUserTS
OS_LOCALE:
USER_LCID:  0
OSBUILD_TIMESTAMP:  2017-09-28 18:32:28
BUILDDATESTAMP_STR:  170928-1534
BUILDLAB_STR:  rs3_release
BUILDOSVER_STR:  10.0.16299.15.x86fre.rs3_release.170928-1534
ANALYSIS_SESSION_ELAPSED_TIME:  162bd
ANALYSIS_SOURCE:  KM
FAILURE_ID_HASH_STRING:  km:av_r_invalid_wwanusbmp!unknown_function
FAILURE_ID_HASH:  {31e4d053-0758-e43a-06a7-55f69b072cb3}
FAILURE_ID_REPORT_LINK: https://go.microsoft.com/fwlink/?
LinkID=397724&FailureHash=31e4d053-0758-e43a-06a7-55f69b072cb3

Followup:     MachineOwner
---------

ReadVirtual: 812d1248 not properly sign extended
```

References

Bug check code reference

Stop error occurs when you update the in-box Broadcom network adapter driver

Article • 10/24/2022 • 2 minutes to read

This issue affects computers that meet the following criteria:

- The operating system is Windows Server 2019, version 1809.
- The network adapter is a Broadcom NX1 Gigabit Ethernet network adapter.
- The number of logical processors is large (for example, a computer that has more than 38 logical processors).

On such a computer, when you update the in-box Broadcom network adapter driver to a later version or when you install the Intel chipset driver, the computer experiences a Stop error (also known as a blue screen error or bug check error).

Cause

The operating system media for Windows Server 2019, version 1809, contains version 17.2 of the Broadcom NIC driver. When you upgrade this driver to a later version, the process of uninstalling the version 17.2 driver generates an error. This is a known issue.

This issue was resolved in Windows Server 2019 version 1903. The operating system media use a later version of the Broadcom network adapter driver.

Workaround

To update the Broadcom network adapter driver on an affected computer, follow these steps:

> ⓘ **Note**
>
> This procedure describes how to use Device Manager to disable and re-enable the Broadcom network adapter. Alternatively, you can use the computer BIOS to disable and re-enable the adapter. For specific instructions, see your OEM BIOS configuration guide.

1. Download the driver update to the affected computer.

2. Open Device Manager, and then select the Broadcom network adapter.
3. Right-click the adapter and then select **Disable device**.
4. Right-click the adapter again and then select **Update driver** > **Browse my computer for driver software**.
5. Select the update that you downloaded, and then start the update.
6. After the update finishes, right-click the adapter and then select **Enable device**.

Generate a kernel or complete crash dump

Article • 09/02/2022 • 3 minutes to read

A system crash (also known as a "bug check" or a "Stop error") occurs when Windows can't run correctly. The dump file that is produced from this event is called a system crash dump.

A manual kernel or complete memory dump file is useful when you troubleshoot several issues because the process captures a record of system memory at the time of a crash.

Applies to: Windows 10

Set up page files

See Support for system crash dumps for the page file size requirement for system crash dump.

Enable memory dump setting

You must be logged on as an administrator or a member of the Administrators group to complete this procedure. If your computer is connected to a network, network policy settings may prevent you from completing this procedure.

To enable memory dump setting, follow these steps:

1. In **Control Panel**, select **System and Security** > **System**.
2. Select **Advanced system settings**, and then select the **Advanced** tab.
3. In the **Startup and Recovery** area, select **Settings**.
4. Make sure that **Kernel memory dump** or **Complete memory dump** is selected under **Writing Debugging Information**.
5. Restart the computer.

> **Note**
>
> You can change the dump file path by edit the **Dump file** field. In other words, you can change the path from *%SystemRoot%\Memory.dmp* to point to a local drive that has enough disk space, such as *E:\Memory.dmp*.

Tips to generate memory dumps

When the computer crashes and restarts, the contents of physical RAM are written to the paging file that is located on the partition on which the operating system is installed.

Depending on the speed of the hard disk on which Windows is installed, dumping more than 2 gigabytes (GB) of memory may take a long time. Even in a best-case scenario, if the dump file is configured to reside on another local hard drive, a significant amount of data will be read and written to the hard disks. This read-and-write process can cause a prolonged server outage.

> **Note**
>
> Use this method to generate complete memory dump files with caution. Ideally, you should do this only when you are explicitly requested to by the Microsoft Support engineer. Any kernel or complete memory dump file debugging should be the last resort after all standard troubleshooting methods have been completely exhausted.

Manually generate a memory dump file

Use the NotMyFault tool

If you can sign in while the problem is occurring, you can use the Microsoft Sysinternals NotMyFault tool by following these steps:

1. Download the NotMyFault tool.
2. Select **Start**, and then select **Command Prompt**.
3. At the command line, run the following command:

```
Console

notMyfault.exe /crash
```

> **Note**
>
> This operation generates a memory dump file and a D1 Stop error.

Use NMI

On some computers, you can't use keyboard to generate a crash dump file. For example, Hewlett-Packard (HP) BladeSystem servers from the Hewlett-Packard Development Company are managed through a browser-based graphical user interface (GUI). A keyboard isn't attached to the HP BladeSystem server.

In these cases, you must generate a complete crash dump file or a kernel crash dump file by using the Non-Maskable Interrupt (NMI) switch that causes an NMI on the system processor.

To implement this process, follow these steps:

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

> **Note**
>
> This registry key isn't required for clients running Windows 8 and later, or servers running Windows Server 2012 and later. Setting this registry key on later versions of Windows has no effect.

1. In Registry Editor, locate the following registry subkey:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl`

2. Right-click **CrashControl**, point to **New**, and then select **DWORD Value**.
3. Type *NMICrashDump*, and then press Enter.
4. Right-click **NMICrashDump**, and then select **Modify**.
5. In the **Value data** box, type *1*, and then select **OK**.
6. Restart the computer.
7. Hardware vendors, such as HP, IBM, and Dell, may provide an Automatic System Recovery (ASR) feature. You should disable this feature during troubleshooting. For example, if the HP and Compaq ASR feature is enabled in the BIOS, disable this

feature while you troubleshoot to generate a complete Memory.dmp file. For the exact steps, contact your hardware vendor.

8. Enable the NMI switch in the BIOS or by using the Integrated Lights Out (iLO) Web interface.

   > **Note**
   >
   > For the exact steps, see the BIOS reference manual or contact your hardware vendor.

9. Test this method on the server by using the NMI switch to generate a dump file. You'll see a STOP 0x00000080 hardware malfunction.

If you want to run NMI in Microsoft Azure using Serial Console, see Use Serial Console for SysRq and NMI calls.

Use the keyboard

Forcing a System Crash from the Keyboard

Use Debugger

Forcing a System Crash from the Debugger

Configure system failure and recovery options in Windows

Article • 09/02/2022 • 9 minutes to read

Applies to: Windows 10

This article describes how to configure the actions that Windows takes when a system error (also referred to as a bug check, system crash, fatal system error, or Stop error) occurs. You can configure the following actions:

- Write an event to the System log.
- Alert administrators (if you've set up administrative alerts).
- Put system memory into a file that advanced users can use for debugging.
- Automatically restart the computer.

> **Note**
>
> You must be logged on as an administrator or a member of the Administrators group to complete this procedure. If your computer is connected to a network, network policy settings may prevent you from completing this procedure.

Configuring system failure and recovery options

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

The options are available in the **Startup and Recovery** dialog box. You can also use the following methods:

- Modify the values under the following registry subkey:

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl`

- To modify the option on your local computer, use the command line utility (*Wmic.exe*) to access Windows Management Instrumentation (WMI).

Follow these steps to view the options in **Startup and Recovery**. (The registry value and Wmic commands are also listed for each option.)

1. In Control Panel, select **System and Security** > **System**.
2. Select **Advanced system settings**, select the **Advanced** tab, and select **Settings** in the **Startup and Recovery** area.

Under "System failure"

Select the check boxes for the actions that you want Windows to perform when a system error occurs.

Write an event to the System log

This option specifies that event information is recorded in the System log. By default, this option is turned on.

To turn off this option, run the following command or modify the registry value:

- Console

```
wmic recoveros set WriteToSystemLog = False
```

- Set the **LogEvent** DWORD value to **0**.

Send an administrative alert

The option specifies that administrators are notified of the system error if you configured administrative alerts. By default, this option is turned on.

To turn off this option, run the following command or modify the registry value:

- Console

```
wmic recoveros set SendAdminAlert = False
```

- Set the **SendAlert** DWORD value to **0**.

Automatically restart

The option specifies that Windows automatically restarts your computer. By default, this option is turned on.

To turn off this option, run the following command or modify the registry value:

- Console

```
wmic recoveros set AutoReboot = False
```

- Set the **AutoReboot** DWORD value to **0**.

Under "Write debugging information"

Select one of the following type of information that you want Windows to record in a memory dump file if the computer stops unexpectedly:

(none)

The option doesn't record any information in a memory dump file.

To specify that you don't want Windows to record information in a memory dump file, run the following command or modify the registry value:

- Console

```
wmic recoveros set DebugInfoType = 0
```

- Set the **CrashDumpEnabled** DWORD value to **0**.

Small Memory Dump

The option records the smallest amount of information to help identify the problem. This option requires a paging file of at least 2 megabytes (MB) on the boot volume of your computer, and specifies that Windows will create a new file each time the system stops unexpectedly. A history of these files is stored in the folder that is listed under Small Dump Directory (*%SystemRoot%\Minidump*). In Windows XP and Windows Server 2003, the small memory dump file is used together with the Windows Error Reporting feature.

To specify that you want to use a small memory dump file, run the following command or modify the registry value:

- Console

```
wmic recoveros set DebugInfoType = 3
```

- Set the **CrashDumpEnabled** DWORD value to **3**.

To specify that you want to use a folder as your Small Dump Directory, run the following command or modify the registry value:

- Console

```
wmic recoveros set MiniDumpDirectory = <folderpath>
```

- Set the **MinidumpDir** Expandable String Value to <folderpath>.

Kernel Memory Dump

The option records only kernel memory. This option stores more information than a small memory dump file, but it takes less time to complete than a complete memory dump file. The file is stored in %SystemRoot%\Memory.dmp by default, and any previous kernel or complete memory dump files are overwritten if the **Overwrite any existing file** check box is selected. If you set this option, you must have a sufficiently large paging file on the boot volume. The required size depends on the amount of RAM in your computer. However, the maximum amount of space that must be available for a kernel memory dump on a 32-bit system is 2 GB plus 16 MB. On a 64-bit system, the maximum amount of space that must be available for a kernel memory dump is the size of the RAM plus 128 MB. The following table provides guidelines for the size of the paging file:

RAM size	**Paging file should be no smaller than**
256 MB–1,373 MB	1.5 times the RAM size
1,374 MB or greater	32-bit system: 2 GB plus 16 MB 64-bit system: size of the RAM plus 128 MB

To specify that you want to use a kernel memory dump file, run the following command or modify the registry value:

- Console

```
wmic recoveros set DebugInfoType = 2
```

- Set the **CrashDumpEnabled** DWORD value to **2**.

To specify that you want to use a file as your memory dump file, run the following command or modify the registry value:

- Console

```
wmic recoveros set DebugFilePath = <filepath>
```

- Set the **DumpFile** Expandable String Value to <filepath>.

To specify that you don't want to overwrite any previous kernel or complete memory dump files, run the following command or modify the registry value:

- Console

```
wmic recoveros set OverwriteExistingDebugFile = 0
```

- Set the **Overwrite** DWORD value to **0**.

Complete Memory Dump

The option records the contents of system memory when the computer stops unexpectedly. This option isn't available on computers that have 2 or more GB of RAM. If you select this option, you must have a paging file on the boot volume that is sufficient to hold all the physical RAM plus 1 MB. The file is stored as specified in *%SystemRoot%\Memory.dmp* by default.

The extra megabyte is required for a complete memory dump file because Windows writes a header in addition to dumping the memory contents. The header contains a crash dump signature and specifies the values of some kernel variables. The header information doesn't require a full megabyte of space, but Windows sizes your paging file in increments of megabytes.

To specify that you want to use a complete memory dump file, run the following command or modify the registry value:

- Console

```
wmic recoveros set DebugInfoType = 1
```

- Set the **CrashDumpEnabled** DWORD value to **1**.

To specify that you want to use a file as your memory dump file, run the following command or modify the registry value:

- Console

```
wmic recoveros set DebugFilePath = <filepath>
```

- Set the DumpFile Expandable String Value to <filepath>.

To specify that you don't want to overwrite any previous kernel or complete memory dump files, run the following command or modify the registry value:

- Console

```
wmic recoveros set OverwriteExistingDebugFile = 0
```

- Set the **Overwrite** DWORD value to **0**.

Automatic Memory Dump

This is the default option. An Automatic Memory Dump contains the same information as a Kernel Memory Dump. The difference between the two is in the way that Windows sets the size of the system paging file. If the system paging file size is set to **System managed size**, and the kernel-mode crash dump is set to **Automatic Memory Dump**, then Windows can set the size of the paging file to less than the size of RAM. In this case, Windows sets the size of the paging file large enough to ensure that a kernel memory dump can be captured most of the time.

If the computer crashes and the paging file isn't large enough to capture a kernel memory dump, Windows increases the size of the paging file to at least the size of RAM. For more information, see Automatic Memory Dump.

To specify that you want to use an automatic memory dump file, run the following command or modify the registry value:

- Console

```
wmic recoveros set DebugInfoType = 7
```

- Set the **CrashDumpEnabled** DWORD value to **7**.

To specify that you want to use a file as your memory dump file, run the following command or modify the registry value:

- Console

```
wmic recoveros set DebugFilePath = <filepath>
```

- Set the **DumpFile** Expandable String Value to <filepath>.

To specify that you don't want to overwrite any previous kernel or complete memory dump files, run the following command or modify the registry value:

- Console

```
wmic recoveros set OverwriteExistingDebugFile = 0
```

- Set the **Overwrite** DWORD value to **0**.

Active Memory Dump

An Active Memory Dump is similar to a Complete Memory Dump, but it filters out pages that are not likely to be relevant to troubleshooting problems on the host machine. Because of this filtering, it's typically significantly smaller than a Complete Memory Dump.

This dump file includes any memory allocated to user-mode applications. It also includes memory allocated to the Windows kernel and hardware abstraction layer, as well as memory allocated to kernel-mode drivers and other kernel-mode programs. The dump includes active pages mapped into the kernel or user space that are useful for debugging, as well as selected Pagefile-backed Transition, Standby, and Modified pages such as the memory allocated with VirtualAlloc or page-file-backed sections. Active dumps don't include pages on the free and zeroed lists, the file cache, guest VM pages, and various other types of memory that are not likely to be useful during debugging. For more information, see Active Memory Dump.

To specify that you want to use an active memory dump file, modify the registry value:

- Set the **CrashDumpEnabled** DWORD value to **1**.
- Set the **FilterPages** DWORD value to **1**.

To specify that you want to use a file as your memory dump file, run the following command or modify the registry value:

- Console

```
wmic recoveros set DebugFilePath = <filepath>
```

- Set the DumpFile Expandable String Value to <filepath>.

To specify that you don't want to overwrite any previous kernel or complete memory dump files, run the following command or modify the registry value:

```
```

- Console

```
wmic recoveros set OverwriteExistingDebugFile = 0
```

- Set the **Overwrite** DWORD value to **0**.

> ⓘ **Note**
>
> If you contact Microsoft Support about a Stop error, you might be asked for the memory dump file that is generated by the Write Debugging Information option.

To view system failure and recovery settings for your local computer, type `wmic recoveros` at a command prompt, and then press Enter. To view system failure and recovery settings for a remote computer on your local area network, type `wmic /node:<computer_name> recoveros` at a command prompt, and then press Enter.

> ⓘ **Note**
>
> To successfully use these *Wmic.exe* command line examples, you must be logged on by using a user account that has administrative rights on the computer. If you are not logged on by using a user account that has administrative rights on the computer, use the `/user:user_name` and `/password:password` switches.

Tips

- To take advantage of the dump file feature, your paging file must be on the boot volume. If you've moved the paging file to another volume, you must move it back to the boot volume before you use this feature.
- If you set the Kernel Memory Dump or the Complete Memory Dump option, and you select the **Overwrite any existing file** check box, Windows always writes to the same file name. To save individual dump files, click to clear the **Overwrite any existing file** check box, and then change the file name after each Stop error.
- You can save some memory if you click to clear the **Write an event to the system log** and **Send an administrative alert** check boxes. The memory that you save depends on the computer, but these features typically require about 60-70 KB.

References

How to determine the appropriate page file size for 64-bit versions of Windows

Article • 09/02/2022 • 8 minutes to read

Page file sizing depends on the system crash dump setting requirements and the peak usage or expected peak usage of the system commit charge. Both considerations are unique to each system, even for systems that are identical. This uniqueness means that page file sizing is also unique to each system and can't be generalized.

Applies to: Windows 10

Determine the appropriate page file size

Use the following considerations for page file sizing for all versions of Windows and Windows Server.

Crash dump setting

If you want a crash dump file to be created during a system crash, a page file or a dedicated dump file must exist and be large enough to back up the system crash dump setting. Otherwise, a system memory dump file isn't created.

For more information, see Support for system crash dumps section.

Peak system commit charge

The system commit charge can't exceed the system commit limit. This limit is the sum of physical memory (RAM) and all page files combined. If no page files exist, the system commit limit is slightly less than the physical memory that is installed. Peak system-committed memory usage can vary greatly between systems. Therefore, physical memory and page file sizing also vary.

Quantity of infrequently accessed pages

The purpose of a page file is to back (support) infrequently accessed modified pages so that they can be removed from physical memory. This removal provides more available space for more frequently accessed pages. The "\Memory\Modified Page List Bytes" performance counter measures, in part, the number of infrequently accessed modified pages that are destined for the hard disk. However, not all the memory on the modified

page list is written out to disk. Typically, several hundred megabytes of memory remains resident on the modified list. Therefore, consider extending or adding a page file if all the following conditions are true:

- More available physical memory (\Memory\Available MBytes) is required.
- The modified page list contains a significant amount of memory.
- The existing page files are fairly full (\Paging Files(*)% Usage).

Support for system crash dumps

A system crash (also known as a "bug check" or a "Stop error") occurs when the system can't run correctly. The dump file that is produced from this event is called a system crash dump. A page file or dedicated dump file is used to write a crash dump file (*Memory.dmp*) to disk. Therefore, a page file or a dedicated dump file must be large enough to support the kind of crash dump selected. Otherwise, the system can't create the crash dump file.

> ⓘ **Note**
>
> During startup, system-managed page files are sized respective to the system crash dump settings. This assumes that enough free disk space exists.

System crash dump setting	Minimum page file size requirement
Small memory dump (256 KB)	1 MB
Kernel memory dump	Depends on kernel virtual memory usage
Complete memory dump	1 x RAM plus 257 MB*
Automatic memory dump	Depends on kernel virtual memory usage. For details, see Automatic memory dump.

* 1 MB of header data and device drivers can total 256 MB of secondary crash dump data.

The Automatic memory dump setting is enabled by default. This setting is an alternative to a kind of crash dump. This setting automatically selects the best page file size, depending on the frequency of system crashes.

The Automatic memory dump feature initially selects a small paging file size. It would accommodate the kernel memory most of the time. If the system crashes again within four weeks, the Automatic memory dump feature sets the page file size as either the RAM size or 32 GB, whichever is smaller.

Kernel memory crash dumps require enough page file space or dedicated dump file space to accommodate the kernel mode side of virtual memory usage. If the system crashes again within four weeks of the previous crash, a Complete memory dump is selected at restart. This dump requires a page file or dedicated dump file of at least the size of physical memory (RAM) plus 1 MB for header information plus 256 MB for potential driver data to support all the potential data that is dumped from memory. Again, the system-managed page file will be increased to back this kind of crash dump. If the system is configured to have a page file or a dedicated dump file of a specific size, make sure that the size is sufficient to back the crash dump setting that is listed in the table earlier in this section together with and the peak system commit charge.

Dedicated dump files

Computers that are running Microsoft Windows or Microsoft Windows Server usually must have a page file to support a system crash dump. System administrators can now create a dedicated dump file instead.

A dedicated dump file is a page file that isn't used for paging. Instead, it is "dedicated" to back a system crash dump file (Memory.dmp) when a system crash occurs. Dedicated dump files can be put on any disk volume that can support a page file. We recommend that you use a dedicated dump file if you want a system crash dump but you don't want a page file. To learn how to create it, see Overview of memory dump file options for Windows.

System-managed page files

By default, page files are system-managed. This system management means that the page files increase and decrease based on many factors, such as the amount of physical memory installed, the process of accommodating the system commit charge, and the process of accommodating a system crash dump.

For example, when the system commit charge is more than 90 percent of the system commit limit, the page file is increased to back it. This surge continues to occur until the page file reaches three times the size of physical memory or 4 GB, whichever is larger. Therefore, it's assumes that the logical disk that is hosting the page file is large enough to accommodate the growth.

The following table lists the minimum and maximum page file sizes of system-managed page files in Windows 10 and Windows 11.

Minimum page file size	Maximum page file size
Varies based on page file usage history, amount of RAM (RAM ÷ 8, max 32 GB) and crash dump settings.	3 × RAM or 4 GB, whichever is larger. This size is then limited to the volume size ÷ 8. However, it can grow to within 1 GB of free space on the volume if necessary for crash dump settings.

Performance counters

Several performance counters are related to page files. This section describes the counters and what they measure.

\Memory\Page/sec and other hard page fault counters

The following performance counters measure hard page faults (which include, but aren't limited to, page file reads):

- \Memory\Page/sec
- \Memory\Page Reads/sec
- \Memory\Page Inputs/sec

The following performance counters measure page file writes:

- \Memory\Page Writes/sec
- \Memory\Page Output/sec

Hard page faults are faults that must be resolved by retrieving the data from disk. Such data can include portions of DLLs, `.exe` files, memory-mapped files, and page files. These faults might or might not be related to a page file or to a low-memory condition. Hard page faults are a standard function of the operating system. They occur when the following items are read:

- Parts of image files (`.dll` and `.exe` files) as they're used
- Memory-mapped files
- A page file

High values for these counters (excessive paging) indicate disk access of generally 4 KB per page fault on x86 and x64 versions of Windows and Windows Server. This disk

access might or might not be related to page file activity but may contribute to poor disk performance that can cause system-wide delays if the related disks are overwhelmed.

Therefore, we recommend that you monitor the disk performance of the logical disks that host a page file in correlation with these counters. A system that has a sustained 100 hard page faults per second experiences 400 KB per second disk transfers. Most 7,200-RPM disk drives can handle about 5 MB per second at an IO size of 16 KB or 800 KB per second at an IO size of 4 KB. No performance counter directly measures which logical disk the hard page faults are resolved for.

\Paging File(*)% Usage

The \Paging File(*)% Usage performance counter measures the percentage of usage of each page file. 100 percent usage of a page file doesn't indicate a performance problem as long as the system commit limit isn't reached by the system commit charge, and if a significant amount of memory isn't waiting to be written to a page file.

> ⓘ **Note**
>
> The size of the Modified Page List (\Memory\Modified Page List Bytes) is the total of modified data that is waiting to be written to disk.

If the Modified Page List (a list of physical memory pages that are the least frequently accessed) contains lots of memory, and if the % Usage value of all page files is greater than 90, you can make more physical memory available for more frequently access pages by increasing or adding a page file.

> ⓘ **Note**
>
> Not all the memory on the modified page list is written out to disk. Typically, several hundred megabytes of memory remains resident on the modified list.

Multiple page files and disk considerations

If a system is configured to have more than one page files, the page file that responds first is the one that is used. This customized configuration means that page files that are on faster disks are used more frequently. Also, whether you put a page file on a "fast" or "slow" disk is important only if the page file is frequently accessed and if the disk that is hosting the respective page file is overwhelmed. Actual page file usage depends greatly

on the amount of modified memory that the system is managing. This dependency means that files that already exist on disk (such as `.txt`, `.doc`, `.dll`, and `.exe`) aren't written to a page file. Only modified data that doesn't already exist on disk (for example, unsaved text in Notepad) is memory that could potentially be backed by a page file. After the unsaved data is saved to disk as a file, it's backed by the disk and not by a page file.

Introduction to page files

Article • 09/02/2022 • 3 minutes to read

A page file (also known as a "paging file") is an optional, hidden system file on a hard disk.

Applies to: Windows 10

Functionality

Page files have the following functionalities.

Physical extension of RAM

Page files enable the system to remove infrequently accessed modified pages from physical memory to let the system use physical memory more efficiently for more frequently accessed pages.

Application requirements

Some products or services require a page file for various reasons. For specific information, check the product documentation.

For example, the following Windows servers require page files:

- Windows Server domain controllers (DCs)
- DFS Replication (DFS-R) servers
- Certificate servers
- ADAM/LDS servers

This requirement is because the algorithm of the database cache for Extensible Storage Engine (ESENT, or ESE for Microsoft Exchange Server) depends on the "\Memory\Transition Pages RePurposed/sec" performance monitor counter. A page file is required to ensure that the database cache can release memory if other services or applications request memory.

For Windows Server 2012 Hyper-V and Windows Server 2012 R2 Hyper-V, the page file of the management OS (commonly called the host OS) should be left at the default of setting of "System Managed".

Support for system crash dumps

Page files can be used to "back" (or support) system crash dumps and extend how much system-committed memory (also known as "virtual memory") a system can support.

For more information about system crash dumps, see system crash dump options.

Page files in Windows with large physical memory

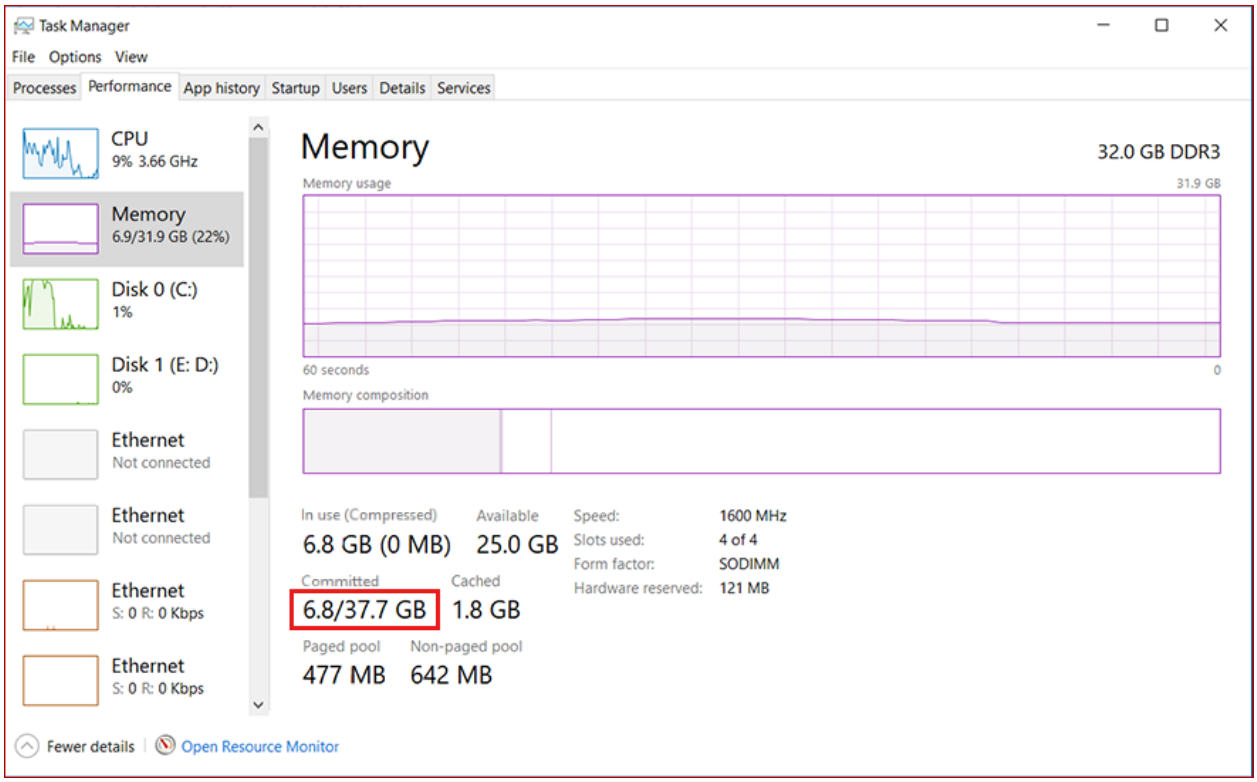
When large physical memory is installed, a page file might not be required to support the system commit charge during peak usage. For example, 64-bit versions of Windows and Windows Server support more physical memory (RAM) than 32-bit versions support. The available physical memory alone might be large enough.

However, the reason to configure the page file size hasn't changed. It has always been about supporting a system crash dump, if it's necessary, or extending the system commit limit, if it's necessary. For example, when a lot of physical memory is installed, a page file might not be required to back the system commit charge during peak usage. The available physical memory alone might be large enough to do this. However, a page file or a dedicated dump file might still be required to back a system crash dump.

System committed memory

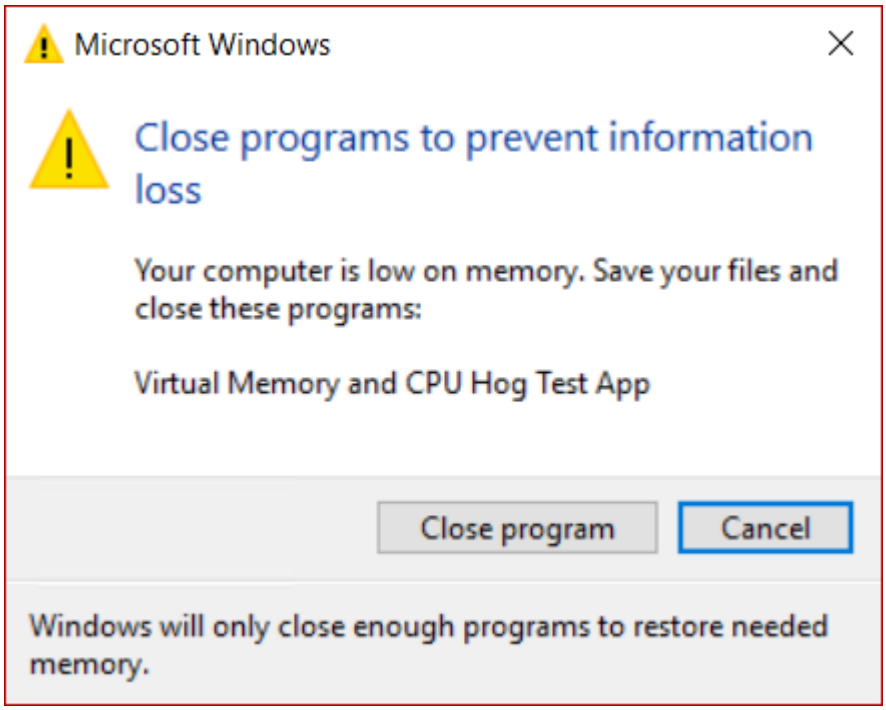
Page files extend how much "committed memory" (also known as "virtual memory") is used to store modified data.

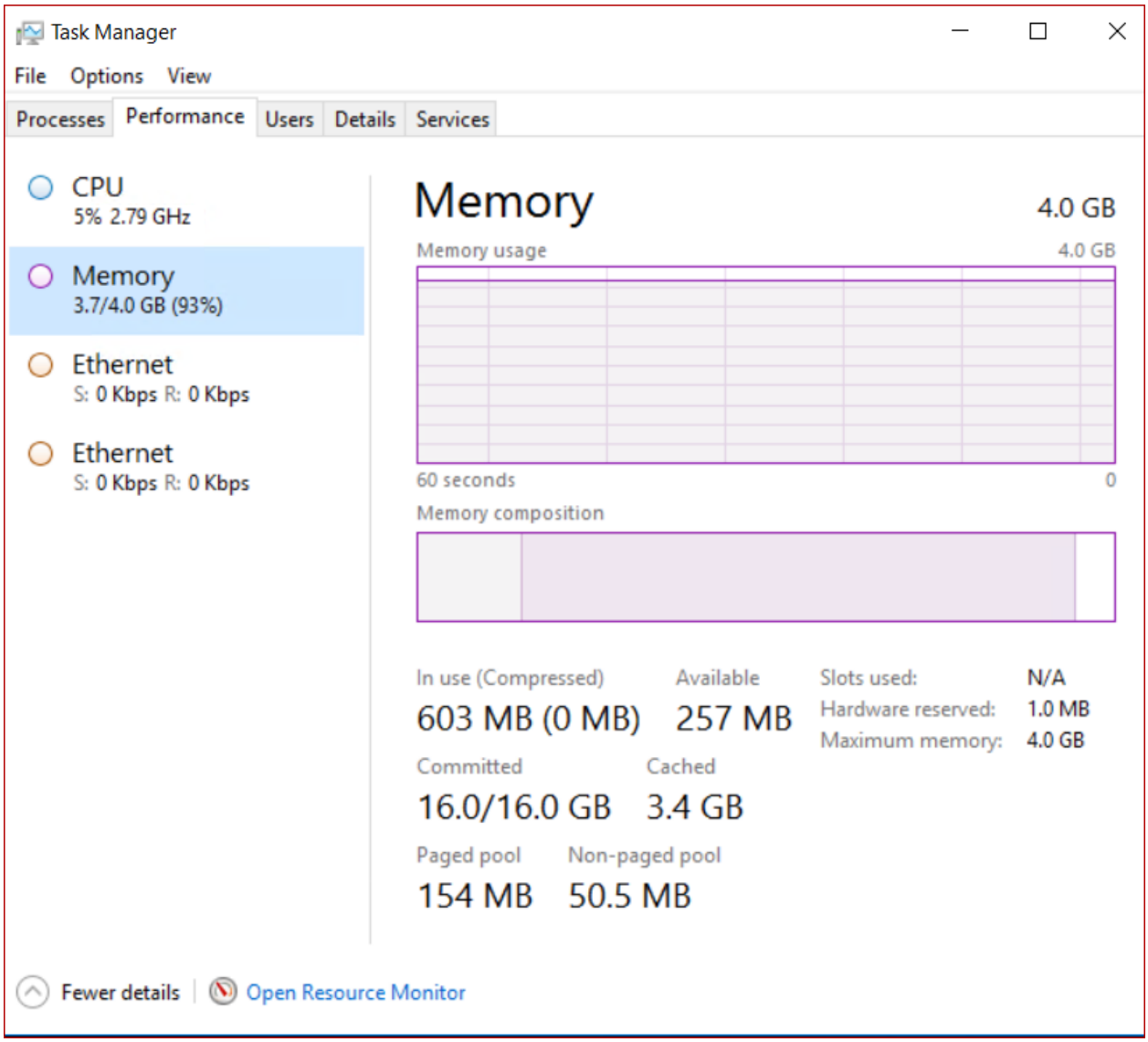
The system commit memory limit is the sum of physical memory and all page files combined. It represents the maximum system-committed memory (also known as the "system commit charge") that the system can support.



> **Note**
>
> In the screenshot, the committed bytes (RAM+Pagefile in use currently) is 6.8 GB and the commit limit (RAM+Pagefile total) is 37.7 GB.

The system commit charge is the total committed or "promised" memory of all committed virtual memory in the system. If the system commit charge reaches the system commit limit, the system and processes might not get committed memory. This condition can cause freezing, crashing, and other malfunctions. Therefore, make sure that you set the system commit limit high enough to support the system commit charge during peak usage.





The system committed charge and system committed limit can be measured on the **Performance** tab in Task Manager or by using the "\Memory\Committed Bytes" and

"\Memory\Commit Limit" performance counters. The \Memory\% Committed Bytes In Use counter is a ratio of \Memory\Committed Bytes to \Memory\Commit Limit values.

> **Note**
>
> System-managed page files automatically grow up to three times the physical memory or 4 GB (whichever is larger, but no more than one-eighth of the volume size) when the system commit charge reaches 90 percent of the system commit limit. This assumes that enough free disk space is available to accommodate the growth.

Stop error 0x113 if you use Intel and AMD graphics adapters on a Windows 8.1-based computer

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where a computer crashes with error code 0x113.

Applies to: Windows 8.1
Original KB number: 2990029

Symptoms

Assume that you have a Windows 8.1-based computer that has a hybrid graphics configuration that uses both Intel and AMD graphics adapters. In this situation, the computer occasionally crashes when it tries to resume from standby, and you receive the following error message: Bug Check 0x113 (VIDEO_DXGKRNL_FATAL_ERROR)

Cause

This issue occurs because the AMD driver does not support Runtime Power Management (RTPM), but the Intel driver does support RTPM.

Workaround

To work around this issue, disable RTPM in the Intel driver.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the "Applies to" section.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

NMI_HARDWARE_FAILURE error when an NMI is triggered on Windows

Article • 09/23/2021 • 2 minutes to read

This article discusses a by-design behavior where the NMI_HARDWARE_FAILURE error occurs when a Non-Maskable Interrupt (NMI) is triggered.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2750146

Symptoms

On a Windows computer, an NMI may be triggered by a user manually pressing an NMI switch on the computer, or because of a hardware error.

In this event, Windows stops executing and displays a bluescreen, stating "Your PC ran into a problem and needs to restart." It includes the following error code: NMI_HARDWARE_FAILURE.

The computer may then save a memory dump file, and may automatically reboot, depending on the settings specified under "Startup and Recovery" in the "Advanced system settings" under the System control panel.

Cause

The behavior when an NMI is encountered has changed compared to earlier versions of Windows. In Windows 7, Windows Server 2008 R2, and earlier versions, the response when the system encountered an NMI was dependent on the configuration of the "NMICrashDump" registry value. For more information about the NMICrashDump registry value and handling of NMIs in earlier Windows versions, click the following article number to view the article in the Microsoft Knowledge Base:
927069 How to generate a complete crash dump file or a kernel crash dump file by using an NMI on a Windows-based system

In Windows 8 and Windows Server 2012, this behavior is not configurable. An NMI will always result in a bugcheck 0x80 (NMI_HARDWARE_FAILURE). This is equivalent to the behavior on earlier Windows versions where the "NMICrashDump" registry value was present and set to a value of 1.

More information

This behavior is by design.

How to read the small memory dump file that is created by Windows if a crash occurs

Article • 03/24/2022 • 6 minutes to read

This article describes how to examine a small memory dump file. A small memory dump file can help you determine why your computer crashed.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 315263

> **Note**
>
> If you are looking for debug information for Windows 8 or later, please check **Debugging Tools for Windows (WinDbg, KD, CDB, NTSD)**. For more information about small memory dump, please check **Small Memory Dump**.

Small memory dump files

If your computer crashes, how can you find out what happened, fix the issue and it prevent it from happening again? You may find the small memory dump file useful in this situation. The small memory dump file contains the smallest amount of useful information that could help you identify why your computer crashed. The memory dump file contains the following information:

- The Stop message, its parameters, and other data
- A list of loaded drivers
- The processor context (PRCB) for the processor that stopped
- The process information and kernel context (EPROCESS) for the process that stopped
- The process information and kernel context (ETHREAD) for the thread that stopped
- The Kernel-mode call stack for the thread that stopped

To create a memory dump file, Windows requires a paging file on the boot volume that is at least 2 megabytes (MB) in size. On computers that are running Microsoft Windows 2000, or a later version of Windows, a new memory dump file is created each time that a computer crash may occur. A history of these files is stored in a folder. If a second problem occurs and if Windows creates a second small memory dump file, Windows

preserves the previous file. Windows gives each file a distinct, date-encoded file name. For example, Mini022900-01.dmp is the first memory dump file that was generated on February 29, 2000. Windows keeps a list of all the small memory dump files in the `%SystemRoot%\Minidump` folder.

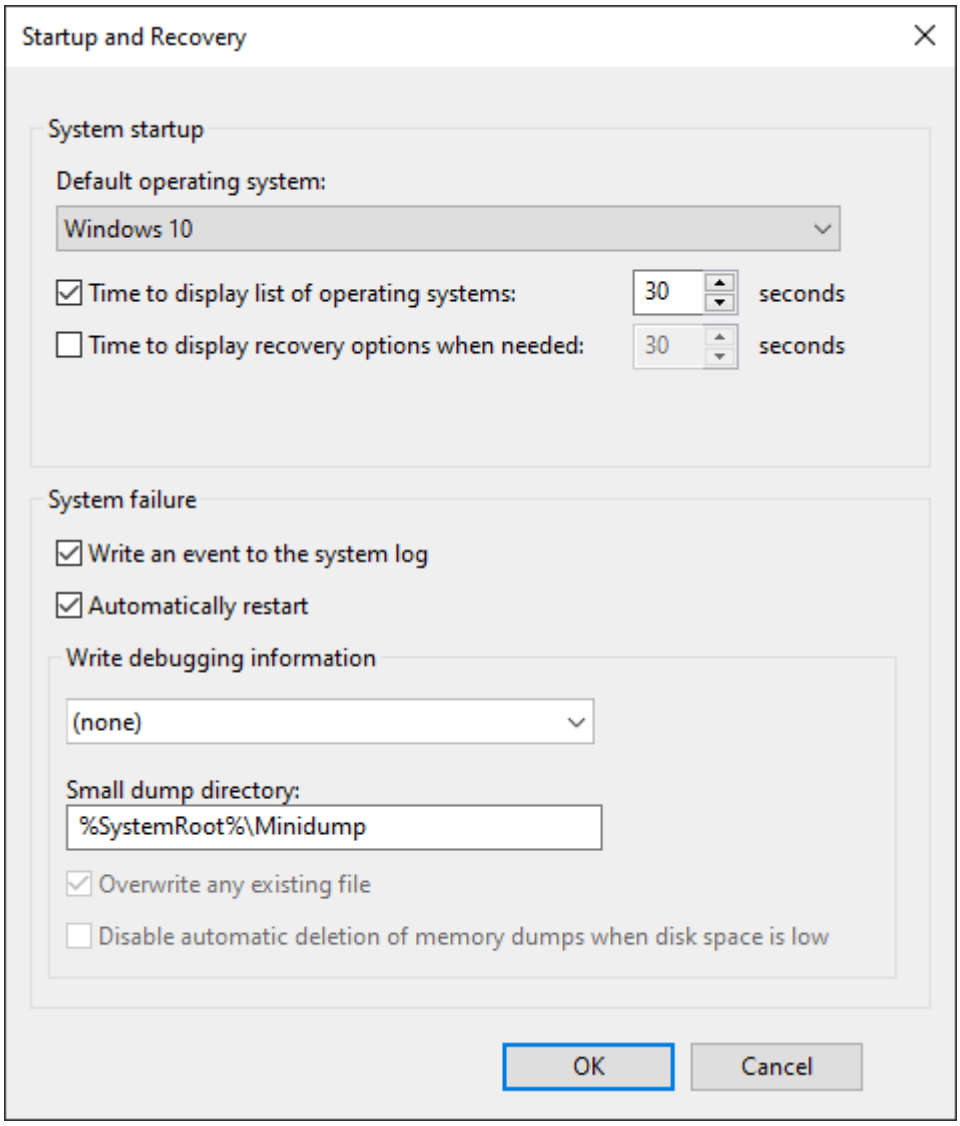
The small memory dump file can be useful when hard disk space is limited. However, because of the limited information that is included, errors that were not directly caused by the thread that was running at the time of the problem may not be discovered by an analysis of this file.

Configure the dump type

To configure startup and recovery options to use the small memory dump file, follow these steps.

> ⓘ **Note**
>
> Because there are several versions of Microsoft Windows, the following steps may be different on your computer. If they are, see your product documentation to complete these steps.

1. Click **Start**, and then click **Control Panel**.
2. Double-click **System**, and then click **Advanced system settings**.
3. Click the **Advanced** tab, and then click **Settings** under **Startup and Recovery**.
4. In the **Write debugging information** list, click **Small memory dump (256k)**.



To change the folder location for the small memory dump files, type a new path in the **Dump File** box or in the **Small dump directory** box, depending on your version of Windows).

Tools to read the small memory dump file

Use the Dump Check Utility (Dumpchk.exe) to read a memory dump file or verify that the file has been created correctly.

> ⓘ **Note**
>
> The Dump Check Utility does not require access to debugging symbols. Symbol files hold a variety of data which are not actually needed when running the binaries, but which could be very useful in the debugging process.

For more information about how to use Dump Check Utility in Windows NT, Windows 2000, Windows Server 2003 or Windows Server 2008, see Microsoft Knowledge Base

article 156280: How to Use Dumpchk.exe to check a memory dump file.

For more information about how to use Dump Check Utility in Windows XP, Windows Vista or Windows 7, see Microsoft Knowledge Base article 315271: How to use Dumpchk.exe to check a Memory Dump file.

Or, you can use the Windows Debugger (WinDbg.exe) tool or the Kernel Debugger (KD.exe) tool to read small memory dump files. WinDbg and KD.exe are included with the latest version of the Debugging Tools for Windows package.

To install the debugging tools, see the Download and Install Debugging Tools for Windows webpage. Select the Typical installation. By default, the installer installs the debugging tools in the following folder:

```
C:\Program Files\Debugging Tools for Windows
```

This Web page also provides access to the downloadable symbol packages for Windows. For more information about Windows symbols, see Debugging with Symbols, and the Download Windows Symbol Packages webpage.

For more information about dump file options in Windows, see Overview of memory dump file options for Windows.

Open the dump file

To open the dump file after the installation is complete, follow these steps:

1. Click **Start**, click **Run**, type `cmd`, and then click **OK**.
2. Change to the Debugging Tools for Windows folder. To do this, type the following at the command prompt, and then press ENTER:

   Console

   ```
   cd c:\program files\debugging tools for windows
   ```

3. To load the dump file into a debugger, type one of the following commands, and then press ENTER:

   Console

   ```
   windbg -y SymbolPath -i ImagePath -z DumpFilePath
   ```

   or

```
Console

kd -y SymbolPath -i ImagePat -z *DumpFilePath
```

The following table explains the use of the placeholders that are used in these commands.

Placeholder	Explanation
SymbolPath	Either the local path where the symbol files have been downloaded or the symbol server path, including a cache folder. Because a small memory dump file contains limited information, the actual binary files must be loaded together with the symbols for the dump file to be correctly read.
ImagePath	The path of these files. The files are contained in the I386 folder on the Windows XP CD-ROM. For example, the path may be `C:\Windows\I386`.
DumpFilePath	The path and file name for the dump file that you are examining.

Sample commands

You can use the following sample commands to open the dump file. These commands assume the following:

- The contents of the I386 folder on the Windows CD-ROM are copied to the `C:\Windows\I386` folder.
- Your dump file is named `C:\Windows\Minidump\Minidump.dmp`.

Sample 1:

```
Console

kd -y srv*c:\symbols*http://msdl.microsoft.com/download/symbols -i
c:\windows\i386 -z c:\windows\minidump\minidump.dmp
```

Sample 2. If you prefer the graphical version of the debugger instead of the command-line version, type the following command instead:

```
Console

windbg -y srv*c:\symbols*http://msdl.microsoft.com/download/symbols -i
c:\windows\i386 -z c:\windows\minidump\minidump.dmp
```

Examine the dump file

There are several commands that you can use to gather information in the dump file, including the following commands:

- The `!analyze -show` command displays the Stop error code and its parameters. The Stop error code is also known as the bug check code.
- The `!analyze -v` command displays verbose output.
- The `lm N T` command lists the specified loaded modules. The output includes the status and the path of the module.

> **Note**
>
> The !drivers extension command displays a list of all drivers that are loaded on the destination computer, together with summary information about their memory use. The !drivers extension is obsolete in Windows XP and later. To display information about loaded drivers and other modules, use the `lm` command. The `lm N T` command displays information in a format that is similar to the old !drivers extension.

For help with other commands and for complete command syntax, see the debugging tools Help documentation. The debugging tools Help documentation can be found in the following location:

`C:\Program Files\Debugging Tools for Windows\Debugger.chm`

> **Note**
>
> If you have symbol-related issues, use the Symchk utility to verify that the correct symbols are loaded correctly. For more information about how to use Symchk, see **Debugging with Symbols**.

Simplify the commands by using a batch file

After you identify the command that you must have to load memory dumps, you can create a batch file to examine a dump file. For example, create a batch file and name it Dump.bat. Save it in the folder where the debugging tools are installed. Type the following text in the batch file:

Console

```
cd "c:\program files\debugging tools for windows"
```

```
kd -y srv*c:\symbols*http://msdl.microsoft.com/download/symbols -i
c:\windows\i386 -z %1
```

When you want to examine a dump file, type the following command to pass the dump file path to the batch file:

Console

```
dump c:\windows\minidump\minidump.dmp
```

Stop code SYSTEM SERVICE EXCEPTION when initializing PMem or NVDIMM in Windows

Article • 11/25/2021 • 2 minutes to read

Applies to: Supported versions of Windows Server and Windows Client

This article provides a method to avoid the stop code SYSTEM SERVICE EXCEPTION when you try to initialize a persistent memory (PMem) or non-volatile dual in-line memory module (NVDIMM) device in Windows.

Stop code when initializing PMem or NVDIMM devices

You create a 64-bit version of Windows virtual machine. Then, you add a persistent memory (PMem) or non-volatile dual in-line memory module (NVDIMM) device with a size less than 16 megabytes (MB) as a PMem disk. When you try to initialize the disk by using the GUID Partition Table (GPT) partition style in **Disk Management**, the initialization fails with this stop code:

> SYSTEM SERVICE EXCEPTION

Use devices with a larger size to avoid this issue

Windows supports PMem or NVDIMM devices (both physical and virtual) with a minimum size of 16 MB. If the size is less than 16 MB, the disk may not be initialized and used.

> ⓘ **Note**
>
> The PMem support in Windows was first introduced in Windows Server 2016 and Windows 10.

To avoid this issue, use a PMem or NVDIMM device with a size of 16 MB or larger.

For more information about creating a persistent memory disk in an unused persistent memory region, see the New-PmemDisk cmdlet.

Stop error 0xE6: DRIVER_VERIFIER_DMA_VIOLATION after repeatedly disabling and enabling a wireless device driver if DMAr is enabled

Article • 09/23/2021 • 2 minutes to read

This article helps to fix the Stop error 0xE6: DRIVER_VERIFIER_DMA_VIOLATION that occurs after you repeatedly disable and enable a wireless device driver.

Applies to: Windows 10, version 2004, Windows 10, version 1909, Windows 10, version 1903
Original KB number: 4576784

Symptoms

You are stress testing or troubleshooting a wireless device driver for an OEM version of Windows 10. The driver uses direct memory access remapping (DMAr).

As part of your testing, you repeatedly disable and enable the wireless driver (for example, in Device Manager). After several such cycles, you notice that the system operations slow down. After 30 minutes of continuously disabling and enabling the driver, the device runs out of memory and stops responding completely.

If you try to use the Driver Verifier tool to analyze the problem, the Windows 10 device experiences a Stop error (also known as a bugcheck or blue screen error). The error code is 0xE6: DRIVER_VERIFIER_DMA_VIOLATION.

Cause

This problem occurs because the DMA adapter allocates memory that is not deallocated correctly when DMA remapping is enabled.

Workaround

> **Important**

You should use this workaround only in a test environment.

To work around this issue, disable DMA remapping by following these steps:

1. Restart the computer, and access the BIOS settings by pressing F10 (or whatever key is designated by the manufacturer) during startup.
2. Select **Advanced** > **System Options**, and then clear the **DMA Protection** setting.

Status

This is a known problem. Microsoft is developing a fix that is scheduled to be included in a future Windows release.

More information

- Enabling DMA remapping for device drivers
- DEVPKEY_Device_DmaRemappingPolicy
- KB 244617: Using Driver Verifier to identify issues with Windows drivers for advanced users
- Bug Check 0xE6: DRIVER_VERIFIER_DMA_VIOLATION

Stop error on Lenovo ThinkPad that has KB4568831 or a later update and Enhanced Windows Biometric Security enabled in UEFI

Article • 09/23/2021 • 2 minutes to read

This article describes a problem that causes a stop error on Lenovo ThinkPad that has KB4568831 or a later update.

Applies to: Windows 10, version 2004
Original KB number: 4580649

Symptoms

You have a Lenovo ThinkPad device that has received the July 31, 2020-KB4568831 (OS Build 19041.423) Preview update or a newer update. The device also has Enhanced Windows Biometric Security enabled in the UEFI, and it runs Lenovo Vantage software.

The device experiences a Stop error (also known as a bugcheck or blue screen error). The codes that are associated with the error are "SYSTEM_THREAD_EXCEPTION_NOT_HANDLED" (in the Stop error message screen) and "0xc0000005 Access Denied" (in memory dumps files and other logs). The associated process is ldiagio.sys.

Cause

Windows devices that receive July 31, 2020-KB4568831 (OS Build 19041.423) Preview or newer updates restrict how processes can access peripheral component interconnect (PCI) device configuration space under specific conditions. Processes that have to access PCI device configuration space must use officially supported mechanisms.

Enabling the Enhanced Windows Biometric Security option in the UEFI of Lenovo ThinkPad devices that were manufactured in 2019 or 2020 meet the conditions that trigger this behavior. When Lenovo Vantage software runs, some versions may try to access PCI device configuration space in an unsupported manner. This action causes a Stop error to occur.

Workaround

To temporarily mitigate this problem, edit the device UEFI configuration (in the **Security** > **Virtualization** section) to disable Enhanced Windows Biometric Security. This change disables the restrictions that are enabled by the SDEV table and VBS.

Status

Lenovo and Microsoft are working on a fix for this problem. For updated Lenovo Vantage support information about this problem, see Lenovo HT511000.

More information

Windows devices that receive the July 31, 2020-KB4568831 (OS Build 19041.423) Preview or later updates restrict how processes can access peripheral component interconnect (PCI) device configuration space if a Secure Devices (SDEV) ACPI table is present and Virtualization-based Security (VBS) is running. Processes that have to access PCI device configuration space must use officially supported mechanisms.

The SDEV table defines secure hardware devices in ACPI. VBS is enabled on a system if security features that use virtualization are enabled. Some examples of these features are Hypervisor Code Integrity or Windows Defender Credential Guard.

The new restrictions are designed to prevent malicious processes from modifying the configuration space of secure devices. Device drivers or other system processes must not try to manipulate the configuration space of any PCI devices, except by using the Microsoft-provided bus interfaces or IRP. If a process tries to access PCI configuration space in an unsupported manner (such as by parsing MCFG table and mapping configuration space to virtual memory), Windows denies access to the process and generates a Stop error.

Enabling the Enhanced Windows Biometric Security option in the UEFI of Lenovo ThinkPad devices that were manufactured in 2019 and 2020 enables an SDEV table. When Lenovo Vantage software runs, some versions may try to access PCI device configuration space in an unsupported manner. This action causes a Stop error. The error is typically displayed as described in the "Symptoms" section.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Third-party contact disclaimer

Microsoft provides third-party contact information to help you find additional information about this topic. This contact information may change without notice. Microsoft does not guarantee the accuracy of third-party contact information.

Tablet device that's running Windows 10 creates only a minidump file

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue that prevents a complete memory dump from being written during a Stop error on a tablet device.

Applies to: Windows 10 - all editions
Original KB number: 3135462

Symptoms

On a tablet device that's running Windows 10 and that uses SD eMMC memory, Windows produces only a minidump file, even if **Kernel memory dump** or **Complete memory dump** is configured under **Advanced System Settings** > **Startup and Recovery**. The minidump file is saved to the %systemroot%\minidump directory instead of to the standard C:\windows\minidump location.

Cause

Because of aggressive power management on SD eMMC devices, Windows always creates a minidump and ignores the memory dump settings that are configured by the administrator. To override this default Windows behavior, special registry settings must be configured.

Resolution

To override the Windows eMMC power-saving feature during a BugCheck (also known as a Stop error or a blue-screen error) to produce a kernel memory dump or a complete memory dump, follow these steps:

1. Under **Advanced System Settings** > **Startup and Recovery**, the **Write debugging information** option must be set to **Kernel memory dump** or **Complete memory dump**.

2. Use Registry Editor to create and configure the following registry key to 0x1 (REG_DWORD) (this permits the dump file to be written):

   ```
   HKLM\SYSTEM\CurrentControlSet\services\sdbus\Parameters\ ForceF0State
   ```

3. Use Registry Editor to create and configure the following registry key. (This makes sure that the dump file isn't deleted upon reboot, even if you're running low on free disk space.)

    - Path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl`
    - Value name: AlwaysKeepMemoryDump
    - Value type: REG_DWORD
    - Value data: 1

4. Make sure that the maximum page file size is larger than the amount of RAM that's being used on the computer. Check this under **Advanced System Settings** > **Performance Option Settings** > **Advanced**. The virtual memory **paging file size** setting on the system drive must be larger than the amount of RAM that's being used.

5. Restart the computer.

Advanced troubleshooting for Windows start-up issues

Article • 10/24/2022 • 2 minutes to read

Try our Virtual Agent - It can help you quickly identify and fix common Windows boot issues

In these articles, you'll learn how to troubleshoot common problems that are related to Windows startup.

How it works

When Microsoft Windows experiences a condition that compromises safe system operation, the system halts. These Windows startup problems are categorized in the following groups:

- Bug check: Also commonly known as a system crash, a kernel error, or a Stop error.
- No boot: The system may not produce a bug check but is unable to start up into Windows.
- Freeze: Also known as "system hang".

Best practices

To understand the underlying cause of Windows startup problems, it's important that the system be configured correctly. Here are some best practices for configuration:

Page file settings

- Introduction of page file
- How to determine the appropriate page file size for 64-bit versions of Windows

Memory dump settings

- Configure system failure and recovery options in Windows
- Generate a kernel or complete crash dump

Troubleshooting

These articles will walk you through the resources you need to troubleshoot Windows startup issues:

- Advanced troubleshooting for Windows boot problems
- Advanced troubleshooting for Stop error or blue screen error
- Advanced troubleshooting for Windows-based computer freeze issues
- Stop error occurs when you update the in-box Broadcom network adapter driver

Advanced troubleshooting for Windows freezes

Article • 09/02/2022 • 10 minutes to read

This article describes how to troubleshoot freeze issues on Windows-based computers and servers. It also provides methods for collecting data that will help administrators or software developers diagnose, identify, and fix these issues.

> **Note**
>
> The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Applies to: Windows 10

Identify the problem

- Which computer is freezing? For example, the affected computer is a physical server or a virtual server.
- What operation happened when it froze? For example, this issue occurs when you shut down.
- How often do the errors occur? For example, this issue occurs every night at 7 PM.
- On how many computers does this freeze occur? For example, all computers or only one computer.

Troubleshoot the freeze issues

To troubleshoot the freeze issues, check the current status of your computer, and follow one of the following methods.

For the computer that's still running in a frozen state

If the physical computer or the virtual machine is still freezing, use one or more of the following methods for troubleshooting:

- Try to access the computer through a remote desktop connection.

- Use a domain account or local administrator account to sign in to the computer with the hardware manufacturer's remote access solution. For example, Dell Remote Access Card (DRAC), HP Integrated Lights-Out (iLo), or IBM Remote supervisor adapter (RSA).
- Test ping to the computer. Look for dropped packets and high network latency.
- Access administrative shares, for example *ServerName*\c$.
- Press Ctrl+Alt+Delete and check the response.
- Try to use Windows remote administration tools. For example, Computer Management, Server Manager, and Wmimgmt.msc.

For the computer that's no longer frozen

If the physical computer or virtual machine froze, but is now running in a good state, use one or more of the following methods for troubleshooting.

For a physical computer

- Review the System and Application logs from the computer that's having the issue. Check the event logs for the relevant Event ID:
  - Application event log: Application Error, which suggests a crash or relevant system process
  - System Event logs, Service Control Manager Error event IDs for critical system services
  - Error Event IDs 2019/2020 with source Srv/Server
- Generate a System Diagnostics report by running `perfmon /report`.

For a virtual machine

- Review the System and Application logs from the computer that is having the issue.
- Generate a System Diagnostics report by running `perfmon /report`.
- Check the system's history in virtual management monitoring tools.

Collect data for the freeze issues

To collect data for a server freeze, check the following table, and use one or more of the suggested methods.

Computer type and state	Data collection method

Computer type and state	Data collection method
A physical computer that's running in a frozen state	Use a memory dump file to collect data. Or use method 2, 3, or 4. These methods are listed later in this section.
A physical computer that is no longer frozen	Use method 1, 2, 3, or 4. These methods are listed later in this section. And use Pool Monitor to collect data.
A virtual machine that's running in a frozen state	Hyper-V or VMware: Use a memory dump file to collect data for the virtual machine that's running in a frozen state. XenServer: Use method 1, 2, 3, or 4. These methods are listed later in this section.
A virtual machine that is no longer frozen	Use method 1, 2, 3, or 4. These methods are listed later in this section.

Method 1: Memory dump

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

A complete memory dump file records all the contents of system memory when the computer stops unexpectedly. A complete memory dump file may contain data from processes that were running when the memory dump file was collected.

If the computer is no longer frozen and now is running in a good state, use the following steps to enable memory dump so that you can collect memory dump when the freeze issue occurs again. If the virtual machine is still running in a frozen state, use the following steps to enable and collect memory dump.

> **Note**
>
> If you have a restart feature that's enabled on the computer, such as the Automatic System Restart (ASR) feature in Compaq computers, disable it. This setting is usually found in the BIOS. With this feature enabled, if the BIOS doesn't detect a heartbeat from the operating system, it will restart the computer. The restart can interrupt the dump process.

1. Make sure that the computer is set up to get a complete memory dump file.
   a. Go to **Run** and enter *Sysdm.cpl*, and then press enter.

b. In **System Properties**, on the **Advanced** tab, select **Performance** > **Settings** > **Advanced**. Select **Change** to check or change the virtual memory.
c. Go back to **System Properties** > **Advanced** > **Settings** in **Startup and Recovery**.
d. In the **Write Debugging Information** section, select **Complete Memory Dump**.
e. Select **Overwrite any existing file**.
f. Make sure that there's a paging file (*pagefile.sys*) on the system drive and that it's at least 100 MB over the installed RAM (Initial and Maximum Size).
g. Make sure that there's more available space on the system drive than there's physical RAM.

2. To allow the system to generate a dump file by using the keyboard, enable the `CrashOnCtrlScroll` registry value.

   a. Open the Registry Editor, and then locate the following registry keys:

      - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters`
      - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kbdhid\Parameters`

   b. Create the following `CrashOnCtrlScroll` registry entry in the two registry keys:

      - Value Name: `CrashOnCtrlScroll`
      - Data Type: **REG_DWORD**
      - Value: **1**

   c. Close the Registry Editor and restart the computer.

3. On some physical computers running earlier versions of Windows, you may generate a nonmakeable interruption (NMI) from a web interface feature such as DRAC, iLo, or RSA. However, by default, this setting will stop the system without creating a memory dump.

   > ⓘ **Note**
   >
   > For currently supported versions of Windows, the `NMICrashDump` registry key is no longer required. An NMI causes a **Stop error that follows a memory dump data collection**.

4. When the computer exhibits the problem, hold down the right Ctrl key, and press the Scroll Lock key two times to generate a memory dump file.

> **Note**
>
> By default, the dump file is located in the following path: *%SystemRoot%\MEMORY.DMP*.

Method 2: Data sanity check

Use the Dump Check Utility (*Dumpchk.exe*) to read a memory dump file. It can also verify that the file was created correctly and isn't corrupted or invalid.

- Using DumpChk
- Download DumpChk

Learn how to use *Dumpchk.exe* to check your dump files:
https://www.youtube-nocookie.com/embed/xN7tOfgNKag

Method 3: Performance Monitor

You can use Windows Performance Monitor to examine how programs that you run affect your computer's performance, both in real time and by collecting log data for later analysis. To create performance counter and event trace log collections on local and remote systems, run the following commands in a command prompt as administrator:

Console

```
Logman create counter LOGNAME_Long -u DOMAIN\USERNAME * -f bincirc -v
mmddhhmm -max 500 -c "\\COMPUTERNAME\LogicalDisk(*)\*"
"\\COMPUTERNAME\Memory\*" "\\COMPUTERNAME\Network Interface(*)\*"
"\\COMPUTERNAME\Paging File(*)\*" "\\COMPUTERNAME\PhysicalDisk(*)\*"
"\\COMPUTERNAME\Process(*)\*" "\\COMPUTERNAME\Redirector\*"
"\\COMPUTERNAME\Server\*" "\\COMPUTERNAME\System\*" "\\COMPUTERNAME\Terminal
Services\*" "\\COMPUTERNAME\Processor(*)\*" "\\COMPUTERNAME\Cache\*" -si
00:05:00
```

Console

```
Logman create counter LOGNAME_Short -u DOMAIN\USERNAME * -f bincirc -v
mmddhhmm -max 500 -c "\\COMPUTERNAME\LogicalDisk(*)\*"
"\\COMPUTERNAME\Memory\*" "\\COMPUTERNAME\Network Interface(*)\*"
"\\COMPUTERNAME\Paging File(*)\*" "\\COMPUTERNAME\PhysicalDisk(*)\*"
"\\COMPUTERNAME\Process(*)\*" "\\COMPUTERNAME\Redirector\*"
"\\COMPUTERNAME\Server\*" "\\COMPUTERNAME\System\*" "\\COMPUTERNAME\Terminal
Services\*" "\\COMPUTERNAME\Processor(*)\*" "\\COMPUTERNAME\Cache\*" -si
00:00:10
```

Then, you can start or stop the log by running the following commands:

```
Console

logman start LOGNAME_Long / LOGNAME_Short
logman stop LOGNAME_Long / LOGNAME_Short
```

The Performance Monitor log is located in the path: *C:\PERFLOGS*.

Other methods to collect data

Use memory dump to collect data for the physical computer that's running in a frozen state

> **⚠ Warning**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

If the physical computer is still running in a frozen state, follow these steps to enable and collect memory dump:

1. Make sure that the computer is set up to get a complete memory dump file and that you can access it through the network.

   > **ⓘ Note**
   >
   > If it isn't possible to access the affected computer through the network, try to generate a memory dump file through NMI. The result of the action may not collect a memory dump file if some of the following settings aren't qualified.

   a. Try to access the desktop of the computer by any means.

   > **ⓘ Note**
   >
   > In case accessing the OS isn't possible, try to remotely access Registry Editor on the computer. You can then check the type of memory dump file and page file with which the computer is currently configured.

b. From a remote computer that's preferably in the same network and subnet, go to **Registry Editor** > **Connect Network Registry**. Then, connect to the affected computer, and verify the following settings:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\CrashDumpEnabled`

  Make sure that the CrashDumpEnabled registry entry is **1**.

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\NMICrashDump`

  On some physical servers, if the NMICrashDump registry entry exists and its value is **1**, you may take advantage of the NMI from the remote management provider such as DRAC, iLo, and RSA.

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PagingFiles and ExistingPageFiles`

  If the value of the `Pagefile` registry entry is system-managed, the size won't be reflected in the registry. For example, `?:\pagefile.sys)`

  If the page file is customized, the size will be reflected in the registry, such as `?:\pagefile.sys 1024 1124`. In this example, 1024 is the initial size and 1124 is the max size.

  > ⓘ **Note**
  >
  > If the size isn't reflected in the Registry, try to access an administrative share where the page file is located. For example, *ServerName**C$*.

c. Make sure that there's a paging file (pagefile.sys) on the system drive of the computer, and it's at least 100 MB over the installed RAM.

d. Make sure that there's more free space on the hard disk drives of the computer than there's physical RAM.

2. Enable the **CrashOnCtrlScroll** registry value on the computer to allow the system to generate a dump file by using the keyboard.

a. From a remote computer preferably in the same network and subnet, go to **Registry Editor** > **Connect Network Registry**. Connect to the affected computer and locate the following registry keys:

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kbdhid\Parameters`

b. Create the following `CrashOnCtrlScroll` registry entry in the two registry keys:

Value Name: `CrashOnCtrlScroll` Data Type: **REG_DWORD** Value: **1**

c. Close the Registry Editor and restart the computer.

3. When the computer exhibits the problem, hold down the right Ctrl key, and press the Scroll Lock key two times to generate a memory dump.

> ⓘ **Note**
>
> By default, the dump file is located in the path: *%SystemRoot%\MEMORY.DMP*.

Use Pool Monitor to collect data for the physical computer that is no longer frozen

Pool Monitor shows you the number of allocations and outstanding bytes of allocation by type of pool and the tag that is passed into calls of ExAllocatePoolWithTag.

For more information, see Using PoolMon to Find a Kernel-Mode Memory Leak and PoolMon Examples.

Use memory dump to collect data for the virtual machine that's running in a frozen state

Use the one of the following methods for the application on which the virtual machine is running.

Microsoft Hyper-V

You can also use the built-in NMI feature through a Debug-VM cmdlet to debug and get a memory dump.

To debug the virtual machines on Hyper-V, run the following cmdlet in Windows PowerShell:

```
```

PowerShell

```
Debug-VM -Name "VM Name" -InjectNonMaskableInterrupt -ComputerName Hostname
```

VMware

You can use VMware snapshots or suspend state and extract a memory dump file equivalent to a complete memory dump file. Use VMware's Checkpoint To Core Tool (vmss2core) to convert both suspend (`.vmss`) and snapshot (`.vmsn`) state files to a dump file. Then analyze the file by using the standard Windows debugging tools.

Citrix XenServer

The memory dump process occurs by pressing the Right Ctrl+Scroll Lock+Scroll Lock keyboard combination. For more information, see Method 1 of How to Trigger a Memory Dump from a Windows Virtual Machine Running on XenServer from Citrix.

Space limitations on the system drive in Windows Server

On a Windows Server, you may not have enough free disk space to generate a complete memory dump file on the system volume.

There's a second option if the system drive doesn't have sufficient space. You can use the DedicatedDumpFile registry entry. For more information, see Configure the destination path for a memory dump.

For more information, see How to use the DedicatedDumpFile registry value to overcome space limitations on the system drive.

Advanced troubleshooting for Windows boot problems

Article • 09/02/2022 • 11 minutes to read

Try our Virtual Agent - It can help you quickly identify and fix common Windows boot issues.

> **Note**
>
> This article is intended for use by support agents and IT professionals. If you're looking for more general information about recovery options, see **Recovery options in Windows 10**.

Applies to: Windows 10

Summary

There are several reasons why a Windows-based computer may have problems during startup. To troubleshoot boot problems, first determine in which of the following phases the computer gets stuck:

Phase	Boot Process	BIOS	UEFI
1	PreBoot	MBR/PBR (Bootstrap Code)	UEFI Firmware
2	Windows Boot Manager	%SystemDrive%\bootmgr	\EFI\Microsoft\Boot\bootmgfw.efi
3	Windows OS Loader	%SystemRoot%\system32\winload.exe	%SystemRoot%\system32\winload.efi
4	Windows NT OS Kernel	%SystemRoot%\system32\ntoskrnl.exe	

1. PreBoot: The PC's firmware initiates a power-on self test (POST) and loads firmware settings. This pre-boot process ends when a valid system disk is detected.

Firmware reads the master boot record (MBR), and then starts Windows Boot Manager.

2. Windows Boot Manager: Windows Boot Manager finds and starts the Windows loader (Winload.exe) on the Windows boot partition.

3. Windows operating system loader: Essential drivers required to start the Windows kernel are loaded and the kernel starts to run.

4. Windows NT OS Kernel: The kernel loads into memory the system registry hive and other drivers that are marked as BOOT_START.

   The kernel passes control to the session manager process (Smss.exe) which initializes the system session, and loads and starts the devices and drivers that aren't marked BOOT_START.

Here's a summary of the boot sequence, what will be seen on the display, and typical boot problems at that point in the sequence. Before you start troubleshooting, you have to understand the outline of the boot process and display status to ensure that the issue is properly identified at the beginning of the engagement. Select the thumbnail to view it larger.



Each phase has a different approach to troubleshooting. This article provides troubleshooting techniques for problems that occur during the first three phases.

> **Note**
>
> If the computer repeatedly boots to the recovery options, run the following command at a command prompt to break the cycle:
>
> `Bcdedit /set {default} recoveryenabled no`
>
> If the F8 options don't work, run the following command:
>
> `Bcdedit /set {default} bootmenupolicy legacy`

BIOS phase

To determine whether the system has passed the BIOS phase, follow these steps:

1. If there are any external peripherals connected to the computer, disconnect them.
2. Check whether the hard disk drive light on the physical computer is working. If it's not working, this dysfunction indicates that the startup process is stuck at the BIOS phase.
3. Press the NumLock key to see whether the indicator light toggles on and off. If it doesn't toggle, this dysfunction indicates that the startup process is stuck at BIOS.

   If the system is stuck at the BIOS phase, there may be a hardware problem.

Boot loader phase

If the screen is black except for a blinking cursor, or if you receive one of the following error codes, this status indicates that the boot process is stuck in the Boot Loader phase:

- Boot Configuration Data (BCD) missing or corrupted
- Boot file or MBR corrupted
- Operating system Missing
- Boot sector missing or corrupted
- Bootmgr missing or corrupted
- Unable to boot due to system hive missing or corrupted

To troubleshoot this problem, use Windows installation media to start the computer, press Shift+F10 for a command prompt, and then use any of the following methods.

Method 1: Startup repair tool

The Startup Repair tool automatically fixes many common problems. The tool also lets you quickly diagnose and repair more complex startup problems. When the computer detects a startup problem, the computer starts the Startup Repair tool. When the tool starts, it performs diagnostics. These diagnostics include analyzing startup log files to determine the cause of the problem. When the Startup Repair tool determines the cause, the tool tries to fix the problem automatically.

To do this task of invoking the Startup Repair tool, follow these steps.

> **Note**
>
> For additional methods to start WinRE, see **Windows Recovery Environment (Windows RE)**.

1. Start the system to the installation media for the installed version of Windows. For more information, see Create installation media for Windows.
2. On the **Install Windows** screen, select **Next** > **Repair your computer**.
3. On the **Choose an option** screen, select **Troubleshoot**.
4. On the **Advanced options** screen, select **Startup Repair**.
5. After Startup Repair, select **Shutdown**, then turn on your PC to see if Windows can boot properly.

The Startup Repair tool generates a log file to help you understand the startup problems and the repairs that were made. You can find the log file in the following location:

%windir%\System32\LogFiles\Srt\Srttrail.txt

For more information, see Troubleshoot blue screen errors.

Method 2: Repair boot codes

To repair boot codes, run the following command:

```
Console

BOOTREC /FIXMBR
```

To repair the boot sector, run the following command:

```
Console

BOOTREC /FIXBOOT
```

> **Note**
>
> Running `BOOTREC` together with `Fixmbr` overwrites only the master boot code. If the corruption in the MBR affects the partition table, running `Fixmbr` may not fix the problem.

Method 3: Fix BCD errors

If you receive BCD-related errors, follow these steps:

1. Scan for all the systems that are installed. To do this step, run the following command:

```
Console

Bootrec /ScanOS
```

2. Restart the computer to check whether the problem is fixed.

3. If the problem isn't fixed, run the following commands:

```
Console

bcdedit /export c:\bcdbackup

attrib c:\boot\bcd -r -s -h

ren c:\boot\bcd bcd.old

bootrec /rebuildbcd
```

4. Restart the system.

Method 4: Replace Bootmgr

If methods 1, 2 and 3 don't fix the problem, replace the Bootmgr file from drive C to the System Reserved partition. To do this replacement, follow these steps:

1. At a command prompt, change the directory to the System Reserved partition.

2. Run the `attrib` command to unhide the file:

```
Console

attrib -r -s -h
```

3. Navigate to the system drive and run the same command:

```
Console

attrib -r -s -h
```

4. Rename the bootmgr file as *bootmgr.old*:

```
Console

ren c:\bootmgr bootmgr.old
```

5. Navigate to the system drive.
6. Copy the bootmgr file, and then paste it to the System Reserved partition.
7. Restart the computer.

Method 5: Restore system hive

If Windows can't load the system registry hive into memory, you must restore the system hive. To do this step, use the Windows Recovery Environment or use the Emergency Repair Disk (ERD) to copy the files from the *C:\Windows\System32\config\RegBack* directory to *C:\Windows\System32\config*.

If the problem persists, you may want to restore the system state backup to an alternative location, and then retrieve the registry hives to be replaced.

> ⓘ **Note**
>
> Starting in Windows 10, version 1803, Windows no longer automatically backs up the system registry to the RegBack folder.This change is by design, and is intended to help reduce the overall disk footprint size of Windows. To recover a system with a corrupt registry hive, Microsoft recommends that you use a system restore point. For more information, see **The system registry is no longer backed up to the RegBack folder starting in Windows 10 version 1803**.

Kernel phase

If the system gets stuck during the kernel phase, you experience multiple symptoms or receive multiple error messages. These error messages include, but aren't limited to, the following examples:

- A Stop error appears after the splash screen (Windows Logo screen).
- Specific error code is displayed. For example, `0x00000C2` , `0x0000007B` , or `inaccessible boot device`.
  - Advanced troubleshooting for Stop error 7B or Inaccessible_Boot_Device
  - Advanced troubleshooting for Event ID 41 "The system has rebooted without cleanly shutting down first"
- The screen is stuck at the "spinning wheel" (rolling dots) "system busy" icon.
- A black screen appears after the splash screen.

To troubleshoot these problems, try the following recovery boot options one at a time.

Scenario 1: Try to start the computer in Safe mode or Last Known Good Configuration

On the **Advanced Boot Options** screen, try to start the computer in **Safe Mode** or **Safe Mode with Networking**. If either of these options works, use Event Viewer to help identify and diagnose the cause of the boot problem. To view events that are recorded in the event logs, follow these steps:

1. Use one of the following methods to open Event Viewer:
    - Go to the **Start** menu, select **Administrative Tools**, and then select **Event Viewer**.
    - Start the Event Viewer snap-in in Microsoft Management Console (MMC).
2. In the console tree, expand Event Viewer, and then select the log that you want to view. For example, choose **System log** or **Application log**.
3. In the details pane, open the event that you want to view.
4. On the **Edit** menu, select **Copy**. Open a new document in the program in which you want to paste the event. For example, Microsoft Word. Then select **Paste**.
5. Use the up arrow or down arrow key to view the description of the previous or next event.

Clean boot

To troubleshoot problems that affect services, do a clean boot by using System Configuration (`msconfig`). Select **Selective startup** to test the services one at a time to determine which one is causing the problem. If you can't find the cause, try including system services. However, in most cases, the problematic service is third-party.

Disable any service that you find to be faulty, and try to start the computer again by selecting **Normal startup**.

For detailed instructions, see How to perform a clean boot in Windows.

If the computer starts in Disable Driver Signature mode, start the computer in Disable Driver Signature Enforcement mode, and then follow the steps that are documented in the following article to determine which drivers or files require driver signature enforcement: Troubleshooting boot problem caused by missing driver signature (x64)

> ⓘ **Note**
>
> If the computer is a domain controller, try Directory Services Restore mode (DSRM).
>
> This method is an important step if you encounter Stop error "0xC00002E1" or "0xC00002E2"

Examples

> ⚠ **Warning**
>
> Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft can't guarantee that these problems can be solved. Modify the registry at your own risk.

> Error code INACCESSIBLE_BOOT_DEVICE (STOP 0x7B)

To troubleshoot this Stop error, follow these steps to filter the drivers:

1. Go to Windows Recovery Environment (WinRE) by putting an ISO disk of the system in the disk drive. The ISO should be of the same version of Windows or a later version.
2. Open the registry.
3. Load the system hive, and name it *test*.
4. Under the following registry subkey, check for lower filter and upper filter items for non-Microsoft drivers:

   `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class`
5. For each third-party driver that you locate, select the upper or lower filter, and then delete the value data.
6. Search through the whole registry for similar items. Process as appropriate, and then unload the registry hive.
7. Restart the server in Normal mode.

For more troubleshooting steps, see Advanced troubleshooting for Stop error 7B or Inaccessible_Boot_Device.

To fix problems that occur after you install Windows updates, check for pending updates by using these steps:

1. Open a Command Prompt window in WinRE.
2. Run the command:

   ```
   Console

   DISM /image:C:\ /get-packages
   ```

3. If there are any pending updates, uninstall them by running the following commands:

   ```
   Console

   DISM /image:C:\ /remove-package /packagename: name of the package

   DISM /Image:C:\ /Cleanup-Image /RevertPendingActions
   ```

   Try to start the computer.

If the computer doesn't start, follow these steps:

1. Open a command prompt window in WinRE, and start a text editor, such as Notepad.
2. Navigate to the system drive, and search for *windows\winsxs\pending.xml*.
3. If the *pending.xml* file is found, rename the file as *pending.xml.old*.
4. Open the registry, and then load the component hive in HKEY_LOCAL_MACHINE as test.
5. Highlight the loaded test hive, and then search for the pendingxmlidentifier value.
6. If the pendingxmlidentifier value exists, delete it.
7. Unload the test hive.
8. Load the system hive, name it *test*.
9. Navigate to the following subkey:

`HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TrustedInstaller`

10. Change the **Start** value from **1** to **4**.
11. Unload the hive.
12. Try to start the computer.

If the Stop error occurs late in the startup process, or if the Stop error is still being generated, you can capture a memory dump. A good memory dump can help determine the root cause of the Stop error. For more information, see Generate a kernel or complete crash dump.

For more information about page file problems in Windows 10 or Windows Server 2016, see Introduction to page files.

For more information about Stop errors, see Advanced troubleshooting for Stop error or blue screen error issue.

Sometimes the dump file shows an error that's related to a driver. For example, *windows\system32\drivers\stcvsm.sys* is missing or corrupted. In this instance, follow these guidelines:

- Check the functionality that's provided by the driver. If the driver is a third-party boot driver, make sure that you understand what it does.
- If the driver isn't important and has no dependencies, load the system hive, and then disable the driver.
- If the stop error indicates system file corruption, run the system file checker in offline mode.
    - To do this action, open WinRE, open a command prompt, and then run the following command:

      Console

      ```
      SFC /Scannow /OffBootDir=C:\ /OffWinDir=C:\Windows
      ```

      For more information, see Using system file checker (SFC) to fix issues.
    - If there's disk corruption, run the check disk command:

      Console

      ```
      chkdsk /f /r
      ```

- If the Stop error indicates general registry corruption, or if you believe that new drivers or services were installed, follow these steps:

    1. Start WinRE, and open a command prompt window.
    2. Start a text editor, such as Notepad.
    3. Navigate to *C:\Windows\System32\Config*.
    4. Rename the all five hives by appending `.old` to the name.
    5. Copy all the hives from the *Regback* folder, paste them in the *Config* folder, and then try to start the computer in Normal mode.

> **Note**
>
> Starting in Windows 10, version 1803, Windows no longer automatically backs up the system registry to the RegBack folder.This change is by design, and is intended to help reduce the overall disk footprint size of Windows. To recover a system with a corrupt registry hive, Microsoft recommends that you use a system restore point. For more information, see **The system registry is no longer backed up to the RegBack folder starting in Windows 10 version 1803**.

Use LiveRE to troubleshoot Windows startup problems

Article • 09/02/2022 • 4 minutes to read

The LiveRE tool creates an image that can be used to start a computer through a USB connection. This tool is helpful in troubleshooting "no boot" issues. It can also be used to provide remote access to a non-starting computer through a jump server for support professionals.

> **Note**
>
> This article is intended for use by support agents and IT professionals.

LiveRE to WinRE comparison

Here is a comparison of Live RE to the existing Windows Recovery Environment that's included with Windows ISOs.

Feature	WinRE/WinPE	iDRAC/ILO	Live operating system (OS)
Availability	With DVD	Special hardware	Flash-drive
Remote Access	No	Yes	Yes
DISM	Yes	Via WinRE	Yes with capability to download missing payloads from internet
DiskPart	Yes	Via WinRE	No, but PowerShell equivalent works
BitLocker	Yes	Via WinRE	Yes
Copy/Paste to allow reduced research and log recording	No	No	Yes
Invoke PowerShell scripts	No	No	Yes
Access to Shadow copies	No	No	Yes

System requirements

- Processor: 1.4Ghz 64-bit processor
- RAM: 512 MB
- Disk Space: 32 GB
- Network: Gigabit (10/100/1000baseT) Ethernet adapter (a 1 Gbps connection is ideal)
- Optical Storage: DVD drive (if installing the OS from DVD media)
- USB 3.0 flash drive, 8 GB or greater
- Video: Super VGA (1024x768) or higher resolution (optional)
- Input Devices: Keyboard and mouse (optional)
- Internet: Broadband access (optional)

Set up the USB flash drive

1. Download the LiveRE image.

2. Connect a USB flash drive.

3. Check whether the nonstarting computer is set up for BIOS startup or UEFI startup. Format the USB drive accordingly:

    - For UEFI:

        Console

        ```
        Diskpart
        List disk
        Sel disk <the number of the flash drive>
        Clean
        Convert gpt
        Create part pri
        Exit
        ```

        Format the partition for the FAT32 file system.

    - For MBR boot:

        Console

        ```
        Diskpart
        List disk
        Sel disk <the number of the flash drive>
        Clean
        Convert mbr
        Create part pri
        List part
        Sel part 1
        ```

```
active
Exit
```

Format the partition for the NTFS file system.

4. Run the following commands:

```
Console

dism /Apply-Image /ImageFile:<complete path of the LiveOS.wim> /Index:1
/ApplyDir:<flash drive letter>:\
<flash drive letter>:\Windows\System32\bcdboot <flash drive
letter>:\Windows /s <flash drive letter>: /f ALL
```

After the USB flash drive is ready, start the affected server from the flash drive.

Create user account for remote access

The following steps help create a user to enable remote access through a jump server:

1. Start the problem computer by using the USB flash drive. Accept the EULA to proceed to the Help console.
2. Press Enter to access PowerShell.
3. Run the following cmdlets:

```
PowerShell

$Password = Read-Host -AsSecureString

New-LocalUser "user_name" -Password $Password
Add-LocalGroupMember -Group "Administrators" -Member "user_name"
```

> **Note**
>
> Enter the password after the first cmdlet.

The computer is now set up for remote access through a jump server. The following screenshot shows a sample cmdlet.

```
1: If no IP is listed, type 1 and hit enter.
2: For instructions to connect from another computer in same network, type 2 and
 hit enter.
3: To Shutdown, type 3 and hit enter.
4: To install drivers in CopyDriversHere folder, type 4 and hit enter.
5: To enter powershell, just hit enter.
Input:

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\windows\system32> $Password = Read-Host -AsSecureString
********
PS C:\windows\system32> New-LocalUser "user_name" -Password $Password

Name      Enabled Description
----      ------- -----------
user_name True


PS C:\windows\system32> Add-LocalGroupMember -Group "Administrators" -Member "us
er_name"
PS C:\windows\system32> _
```

Connect from the jump server

1. Get the IP address from the LiveRE screen.

```
**************************
     Welcome to Live RE
**************************
Please check you ip address below

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : fe80::2479:3ed9:45ba:8615%3
   IPv4 Address. . . . . . . . . . . : 172.25.80.68
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . : 172.25.80.1
If IP address is blank, verify if network card is enabled by running the command
 'Get-Netadapter' on powershell

1: If no IP is listed, type 1 and hit enter.
2: For instructions to connect from another computer in same network, type 2 and
 hit enter.
3: To Shutdown, type 3 and hit enter.
4: To install drivers in CopyDriversHere folder, type 4 and hit enter.
5: To enter powershell, just hit enter.
Input: _
```

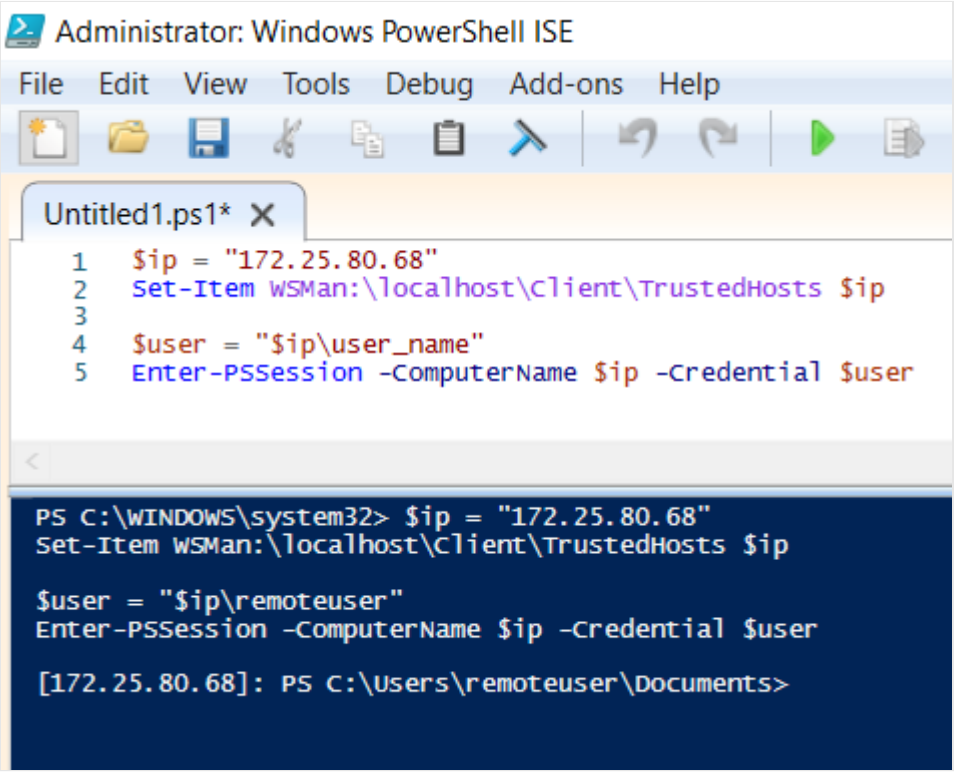
2. On a working computer in the same network as the nonstarting computer, open PowerShell ISE, and run the following script:

PowerShell

```
$ip = "172.25.80.68"
Set-Item WSMan:\localhost\Client\TrustedHosts $ip
$user = "$ip\user_name"
Enter-PSSession -ComputerName $ip -Credential $user
```

3. When prompted, enter the password.

4. You will be connected to the broken computer through WinRM.



If you experience issues when you connect through WinRM, check whether WinRM is enabled. If it isn't, run the `winrm qc` command to enable WinRM.

If you receive an error message that reassembles the following message, this means that the network connections is set to **Public**.

```
C:\WINDOWS\system32>ncpa.cpl

C:\WINDOWS\system32>winrm qc
WinRM service is already running on this machine.
WSManFault
    Message
        ProviderFault
            WSManFault
                Message = WinRM firewall exception will not work since one of the network connection types on this machi
ne is set to Public. Change the network connection type to either Domain or Private and try again.

Error number:  -2144108183 0x80338169
WinRM firewall exception will not work since one of the network connection types on this machine is set to Public. Chang
e the network connection type to either Domain or Private and try again.

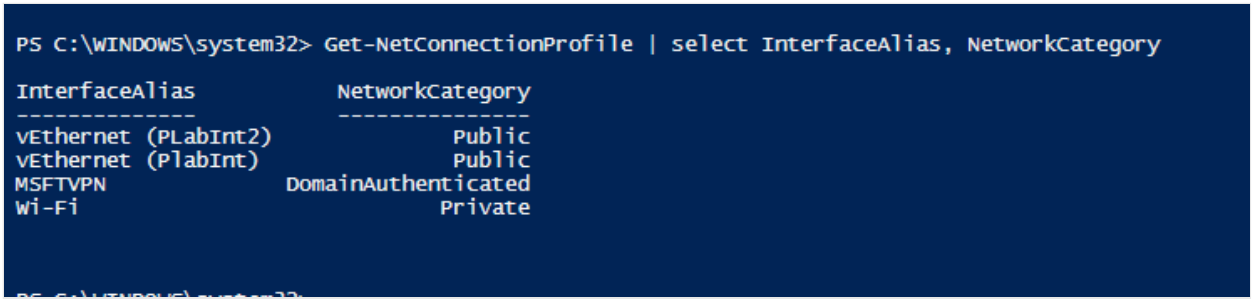
C:\WINDOWS\system32>
```

You can determine which connections are set to **Public** by running the following cmdlet:

PowerShell

```
Get-NetConnectionProfile | select InterfaceAlias, NetworkCategory
```

The following is a sample output:



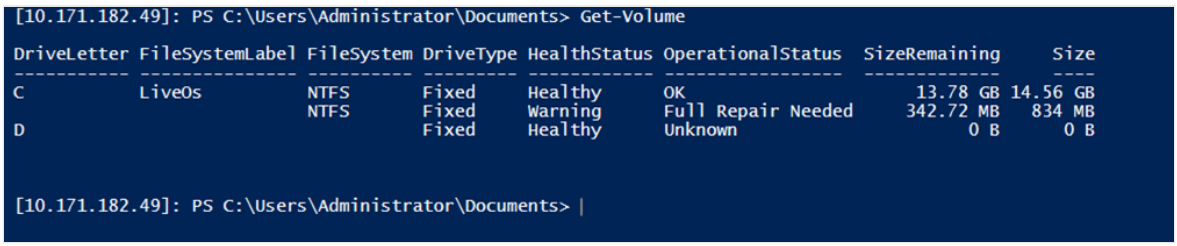
You can either disable the public connections or change them to private after you remove permissions from the customer. To do this, run the following cmdlet:

PowerShell

```
Set-NetConnectionProfile -interfacealias "vEthernet (Internal LAN)" -
NetworkCategory Private
```

Unlock BitLocker drives from LiveRE

1. Run `Get-Volume` to find the drive letter:



2. Run the following command:

   PowerShell

   ```
   Unlock-BitLocker -MountPoint <drive letter> -RecoveryPassword <recovery
   password>
   ```

Disk configuration

Because *Diskpart.exe* is not available in LiveRE, use PowerShell to achieve similar results. Here are a few commands:

1. Check Disk: `Get-Disk`
2. Check partitions in a disk: `Get-Partition -DiskNumber <number>`
3. Set a partition to active: `Set-Partition -DiskNumber <number> -PartitionNumber <number> -IsActive $true`
4. Check properties of a partition: `Get-Partition -DiskNumber <number> -PartitionNumber <number> |fl`

For more information, see Windows Storage Management-specific cmdlets.

Registry configuration

There is no registry editor is Live OS. In order to change the registry, access the share for affected OS drive by using the *<IP Address>*\c$ path.

Get the hives from *\windows\system32\config*, make the changes to the hives, and then continue to the next steps.

Access shadow copies

LiveRE allows access to shadow copies from disks of a computer that is not starting, this can be used to replace previous versions of files.

You can use the following steps to access previous versions of the files:

PowerShell

```
Get-CimInstance -ClassName Win32_ShadowCopy | select
volumename,ID,InstallDate,DeviceObject
Get-Volume | select Driveletter,path to get the volume name association with
Volume ID
```

> **Note**
>
> The OS date and time have to be adjusted per the correct time zone to remain accurate. LiveOS uses the Coordinated Universal Time (Greenwich Mean Time) time zone.

Copy the DeviceObject for the shadow copy that you want to access, and then run the following commands:

Console

```
$sobj="<DeviceObject>" + "\"
cmd /c mklink /d c:\shadowcopy "$sobj"
```

You can now access the previous versions of the file from PowerShell by browsing to *<IP>*\c$\shadowcopy.

Injecting drivers

If you have a RAID-disk setup, you have to install RAID drivers from OEM media to make the volumes visible to the OS.

In LiveRE, you can extract the RAID drivers to the *<USB>*:*CopyDriversHere* folder.

Then, after you start in LiveRE, press the 4 key to install the drivers.

Another way to install drivers is to do the following:

1. Download and extract the drivers to a folder on the LiveRE flash drive.
2. After you connect to the affected conputer, run the following cmdlet:

   PowerShell

   ```
   pnputil /add-driver <location of raid driver.inf>

   Add-WindowsDriver -Path <flash drive letter>:\ -Driver <path of driver
   folder> -Recurse
   ```

Unable to refresh or reset PC after Automatic Repair fails in Windows 8

Article • 09/23/2021 • 2 minutes to read

This article fixes an issue in which you cannot refresh or reset the PC after Automatic Repair fails.

Applies to: Windows 8
Original KB number: 2823223

Symptoms

Consider the following scenario:

- You have Windows 8 or Windows 8 Pro installed on your PC.
- Your PC fails to boot into Windows and launches Automatic Repair to attempt to repair Windows.
- Automatic Repair is unable to repair your PC and you select **Advanced options**.
- After selecting **Troubleshoot**, you choose to either **Refresh your PC** or **Reset your PC**.

In this scenario, recovery may fail and you're returned back to the main WinRE screen.

Cause

This issue may occur if the System or Software registry hives have become damaged or corrupted.

Resolution

To attempt to resolve this issue, follow the steps below.

> ⓘ **Note**
>
> These steps should only be used if you're attempting to use the **Refresh your PC** or **Reset your PC** options in Windows RE because your system is in a non-bootable state.

1. After Automatic Repair fails to repair your PC, select **Advanced options** and then **Troubleshoot**.
2. Select **Advanced options** and then select Command Prompt.
3. If prompted, enter in the password for the user name.
4. At the Command Prompt, go to the \windows\system32\config folder by typing the following command:

   ```
   Console

   cd %windir%\system32\config
   ```

5. Rename the System and Software registry hives to System.001 and Software.001 by using the following commands:

   ```
   Console

   ren system system.001
   ren software software.001
   ```

   > **Note**
   >
   > Renaming the Software hive won't allow you to use the "Refresh your PC" option. If you want to use the "Refresh your PC" option, only rename the System hive. If the Software hive is also corrupt, you may not be able to use the "Refresh your PC" option.

6. Type *exit* without the quotes to exit the Command Prompt and reboot the PC back to the Automatic Repair screen.
7. After selecting **Advanced options** and then **Troubleshoot**, select either **Refresh your PC** or **Reset your PC**.

More information

Using the **Reset your PC** option will remove all of the files on your hard drive and resets your PC back to the version of Windows 8 that was preinstalled by the OEM on your PC. All new applications that were installed on your PC after you purchased it will need to be reinstalled.

Can't start Windows 11 in S mode from a recovery drive

Article • 11/22/2021 • 2 minutes to read

Windows 11 in S mode has security policies that ensure the system runs securely. When you try to start Windows 11 in S mode from a recovery drive, the system may fail to start because of a missing policy. To work around this issue, you can copy the policy file to a designated location of the drive by using one of the following methods.

Copy the policy file from the recovery drive

Follow these steps to check whether the recovery drive includes the policy file, and then copy the file to a designated location of the drive.

1. Insert or connect the recovery drive to your computer.
2. Open **File Explorer**, go to the *<Recovery Drive>:\EFI\Microsoft\Boot* folder, and check if the *winsipolicy.p7b* file is in the folder.
3. If the *winsipolicy.p7b* file is in the folder, copy the file to the *<Recovery Drive>:\EFI\Boot* folder.

Copy the policy file from another Windows computer

If the recovery drive doesn't include the policy file, copy the file from another Windows computer.

1. Insert or connect the recovery drive to another Windows computer.
2. Open **File Explorer**, go to the *C:\Windows\Boot\EFI* folder, and copy the *winsipolicy.p7b* file to the *<Recovery Drive>:\EFI\Boot* folder.

Status

This issue will be resolved in a future Windows servicing update, and this article will be updated when the servicing update is released.

Changing the ATA Drive setting in System Bios causes reboot loop

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to a reboot loop issue that's caused by changing the ATA Drive setting.

Applies to: Windows 8
Original KB number: 2751461

Symptoms

Consider the following scenario:

- The BIOS setting for the drive is set to ATA Mode.
- Install or upgrade the system to Windows 8.
- You boot into the BIOS and changed the ATA setting from ATA Mode to AHCI Mode pressed enter to accept the change.
- You click Yes to the Warning about the detected mode change on the embedded ATA controller.
- You restart the computer and boot normally. In this scenario, during the system boot when Windows tries to start, you will receive an error with regards to a system failure. The system will be stuck in a reboot loop.

Cause

This is due to changes in Windows 8 PnP in which Boot Start Drivers are not installed by default.

Resolution

In order to correct this issue, please walk through the following steps:

1. Power down or restart the computer and enter the system BIOS.
2. Change the ATA Drive setting back to ATA Mode, press enter to accept the change and restart the computer.
3. Click Yes to the Warning about the detected mode change on the embedded ATA controller.

4. The system will boot normally to the Modern App Start Menu.

> **Note**
>
> Be sure you know the Local Admin account and password and are able to boot successfully before proceeding.

5. Open an elevated command prompt and run the following command to enable SafeMode boot: bcdedit /set {current} safeboot minimal
6. Restart the computer and boot to the system BIOS.
7. Change the ATA Drive setting from ATA Mode to AHCI Mode, press enter to accept the change.
8. Click Yes to the Warning about the detected mode change on the embedded ATA controller.
9. The system will boot normally to the Modern App Start Menu in SafeMode.
10. Open an elevated command prompt and run the following command to remove the SafeMode boot option:

```
Console
bcdedit /deletevalue {current} safeboot
```

11. Restart the computer and boot normally, the system will boot successfully to the Modern App Start Menu.

More information

For additional information on Windows 7 in a similar scenario, please see the following KB.

Error message when you start a Windows 7 or Windows Vista-based computer after you change the SATA mode of the boot drive: "STOP 0x0000007B INACCESSABLE_BOOT_DEVICE"https://support.microsoft.com/kb/922976

Invalid Boot File Received Error Message When PXE booting from WDS

Article • 09/23/2021 • 2 minutes to read

This article provides help to fix an error that occurs when you use PXE to boot a client computer from a Windows Deployment Services (WDS) server.

Applies to: Windows 10 - all editions
Original KB number: 2602043

Symptoms

When using PXE to boot a client computer from a WDS server, you may encounter one of the following symptoms or error messages

- Invalid boot file received
- PXE client hangs. At the point of the error you are executing code from the PXE bios, so the actual error message can vary.

Cause

This can occur with the following scenario:

- You are using DHCP scope option 67 to direct PXE clients to download specific Boot Program using BootFileName.
- You have a mix of BIOS-based machines and UEFI machines and you attempt to boot the incorrect type of Boot Program

Resolution

If you have a mix of UEFI and Legacy BIOS machines, you cannot use DHCP Scope Options to direct PXE clients to the Boot Program on the WDS server. You must use IP Helper Table Entries. For more information on configuring IP helper table entries, contact your router/switch manufacturer.

More information

The WDS Boot Program's for each type of machine are:

- Legacy BIOS computers: Wdsnbp Website
- UEFI computers: wdsmgfw.efi Managing Network Boot Programs

PROCESS1_INITIALIZATION_FAILED stop error after you upgrade to Windows 10 Version 1607

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround to an issue that triggers a stop error on a blue screen after you upgrade your system to Windows 10 Version 1607.

Applies to: Windows 10, version 1607
Original KB number: 3083796

Symptoms

After you perform an upgrade to Windows 10 Version 1607 from Windows 7, Windows 8, or Windows 8.1, the system fails to start, and you receive a "PROCESS1_INITIALIZATION_FAILED" error message.

Cause

This issue occurs if you have the HIBUN application from Hitachi installed. Hitachi HIBUN is incompatible with a compression technology in Windows 10 Version 1607. To prevent data corruption, Windows fails to start after a Windows 10 upgrade in this scenario.

Workaround

To work around this issue, roll back the system to the previous OS, uninstall Hitachi HIBUN, and then upgrade to Windows 10 Version 1607. To do this, follow these steps:

1. Reboot the computer, and wait for the Windows Recovery Environment (WinRE) to start.
2. Click **Troubleshoot**, select **Advanced Options**, and then select **Go back to the previous build**.
3. Uninstall Hitachi HIBUN.
4. Upgrade to Windows 10 Version 1607.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Windows devices may fail to boot after installing October 10 version of KB4041676 or KB4041691 that contained a publishing issue

Article • 12/06/2021 • 4 minutes to read

This article provides workarounds for the issue where Windows devices may fail to boot after installing October 10 version of KB4041676 or KB4041691.

Applies to: Windows Server 2016, Windows 10, version 1607, Windows 10, version 1703
Original KB number: 4049094

Overview

Microsoft is aware of a publishing issue with the October 10, 2017 monthly security updates for Windows 10 version 1703 (KB4041676) and version 1607 (KB4041691), and Windows Server 2016 (KB4041691) for WSUS/SCCM managed devices. Customers that download updates directly from Windows Update (Home and consumer devices) or Windows Update for Business are not impacted.

We have corrected the publishing issue as of the afternoon of October 10 and have validated the cumulative security updates. We recommend all customers take these cumulative security updates.

We have reports of the following symptoms impacting Windows Server Update Services (WSUS) and System Center Configuration Manager (SCCM) customers. Mitigation plans for the following user reported scenarios can be found below.

1. WSUS/SCCM Administrators that synced the October 10 update (KB4041676 or KB4041691) before 4pm PDT October 10 may still have these KBs cached.
2. WSUS/SCCM managed devices that downloaded the October 10 KB4041676 or KB4041691 update with publishing issues and have devices in a pending reboot state.
3. WSUS/SCCM managed devices that installed the October 10 KB4041676 or KB4041691 update and are unable to boot and/or may land on a recovery screen.

Issue details

Scenario 1

WSUS/SCCM Administrators that synced the Delta Package versions of KB4041676 or KB4041691 before 4pm PDT October 10 may still have these KBs cached.

Workaround

WSUS/SCCM administrators should rescan for updates to automatically resolve the publishing issue. The issue is already resolved in WSUS hierarchies that have scanned since 4PM on October 10. Ensure your upstream and downstream servers are in sync.

Scenario 2

WSUS/SCCM managed devices that have downloaded and staged the Delta Package versions of KB4041676 or KB4041691 but have not rebooted to install.

Workaround

If a device has downloaded and staged Delta Package versions of KB4041676 or KB4041691, a user may fail to boot after restarting. System administrators can remove pending updates by running the following commands from an administrative command prompt on the device:

Console

```
@echo off

REM Stop all update related services
net stop usosvc
net stop wuauserv
net stop trustedinstaller

REM Delete pending.xml if it exists
takeown /f %windir%\winsxs\pending.xml >NUL 2>&1
icacls %windir%\winsxs\pending.xml /grant Everyone:F >NUL 2>&1
del %windir%\winsxs\pending.xml >NUL 2>&1

REM Modify the components hive
reg unload HKLM\Components >NUL 2>&1
reg load HKLM\ComponentsHive %windir%\system32\config\COMPONENTS
reg delete /f HKLM\ComponentsHive /v PendingXmlIdentifier >NUL 2>&1
reg delete /f HKLM\ComponentsHive /v PoqexecFailure >NUL 2>&1
reg delete /f HKLM\ComponentsHive /v ExecutionState >NUL 2>&1
reg delete /f HKLM\ComponentsHive /v RepairTransactionPended >NUL 2>&1
reg delete /f HKLM\ComponentsHive /v AIFailureInformation >NUL 2>&1
reg delete /f HKLM\ComponentsHive\Installers\RegKeySDTable /v Install >NUL
2>&1
```

```
reg delete /f HKLM\ComponentsHive\Installers\RegKeySDTable /v Uninstall >NUL
2>&1
reg delete /f HKLM\ComponentsHive\Installers\RegKeySDTable /v Uninstall >NUL
2>&1
reg unload HKLM\ComponentsHive

REM Stop Poqexec from running
reg delete /f
HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide\Configuration /v
DontRunPoqexecInSmss >NUL 2>&1
reg delete /f
HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide\Configuration /v
PoqexecCmdline >NUL 2>&1
reg delete /f "HKLM\System\CurrentControlSet\Control\Session Manager" /v
SETUPEXECUTE >NUL 2>&1
REG ADD "HKLM\System\CurrentControlSet\Control\Session Manager" /v
SETUPEXECUTE /t REG_MULTI_SZ /d \0 /f

dism /online /remove-package
/PackageName:Package_for_RollupFix_Wrapper~31bf3856ad364e35~amd64~~15063.674
.1.8 /norestart >NUL 2>&1
dism /online /remove-package
/PackageName:Package_for_RollupFix_Wrapper~31bf3856ad364e35~x86~~15063.674.1
.8 /norestart >NUL 2>&1
dism /online /remove-package
/PackageName:Package_for_RollupFix_Wrapper~31bf3856ad364e35~amd64~~14393.177
0.1.6 /norestart >NUL 2>&1
dism /online /remove-package
/PackageName:Package_for_RollupFix_Wrapper~31bf3856ad364e35~x86~~14393.1770.
1.6 /norestart >NUL 2>&1
```

Scenario 3

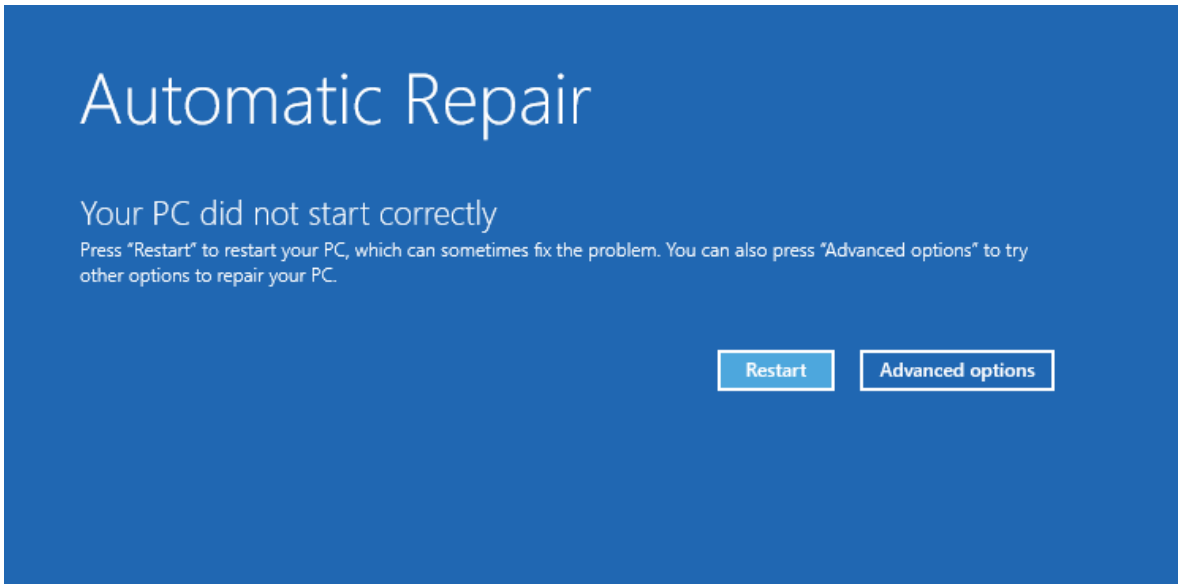
WSUS/SCCM managed devices that installed the Delta Package versions of KB4041676 or KB4041691 and are unable to boot and/or see a recovery screen

Workaround

> ⓘ **Important**

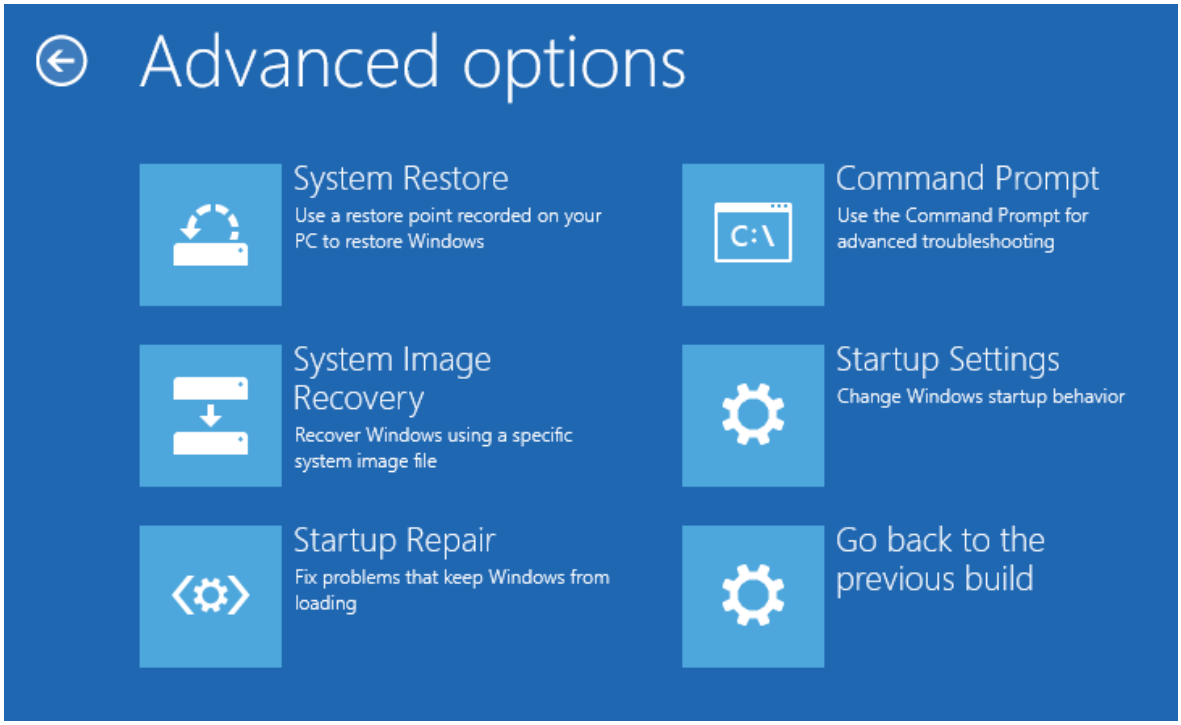
These steps should only be followed on a device that fails to boot.

1. Plug into AC power and turn on the device.
2. If the device fails to boot, Windows will attempt to repair your device and enter the Windows 10 Recovery Environment. Select **Advanced options** on the **Automatic Repair** screen.



3. Select **Troubleshoot**, then **Advanced Options**, and then **System Restore**. If a restore point is available prior to the installation of KB4041676 or KB4041691, use the **System Restore** wizard to restore to the earlier Restore Point. If a restore point does not exist, close **System Restore** and continue to the next step.

4. Select **Troubleshoot**, then **Advanced Options** and then **Command Prompt**. You may be asked to enter a BitLocker Recovery Key or username/password. If prompted for a username/password, you must enter a local account. If you do not have credentials, you many need to create and use a Recovery Drive.



5. After the **Command Prompt** launches, run the following to load the software registry hive:

```
Console
```

```
reg load hklm\temp <drive letter for windows
directory>\windows\system32\config\software
```

Example:

```
Console

reg load hklm\temp c:\windows\system32\config\software
```

6. Run the following command to delete the SessionsPending registry key. If the registry value does not exist, proceed to the next step.

```
Console

reg delete "HKLM\temp\Microsoft\Windows\CurrentVersion\Component Based
Servicing\SessionsPending" /v Exclusive
```

7. Run the following to unload the registry:

```
Console

reg unload HKLM\temp
```

8. Run the following command, which will list all pending updates:

```
Console

dism.exe /image:<drive letter for windows directory> /Get-Packages
```

Example:

```
Console

dism.exe /image:c:\ /Get-Packages
```

9. Run the following command for each package where State = Install Pending:

```
Console

dism.exe /image:<drive letter for windows directory> /remove-package
/packagename:<package name>
```

Example:

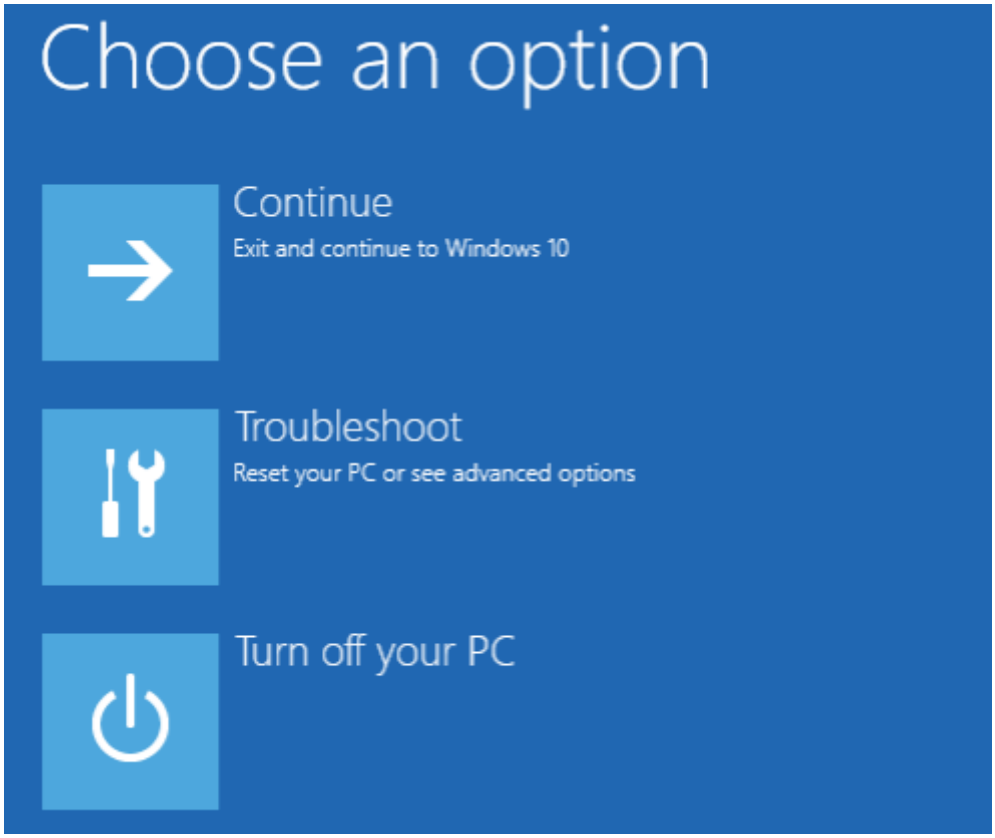
Console

```
dism.exe /image:c:\ /remove-package
/packagename:Package_for_RollupFix_Wrapper~31bf3856ad365e35~amd64~~1506
3.674.1.8
```

Console

```
dism.exe /image:c:\ /remove-package
/packagename:Package_for_RollupFix~31bf3856ad365e35~amd64~~15063.674.1.
8
```

10. Close the **Command Prompt** and click **Continue** to exit the recovery environment.



Windows fails to start with error missing or corrupt ntoskrnl.exe when keys are pressed during startup

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for the issue Windows fails to start with error missing or corrupt ntoskrnl.exe when keys are pressed during startup.

Applies to: Windows 10 - all editions
Original KB number: 2022960

Symptoms

When you press or hold down keys on the keyboard as you start your computer, you may see the following message and Windows will fail to start.

> Windows could not start because the following file is missing or corrupt:
> <Windows root>\system32\ntoskrnl.exe.
> Please re-install a copy of the above file.

This problem does not occur if you do not press any keys during startup.

> **Note**
>
> This problem can occur on any Windows operating system prior to Windows 7, on both 32-bit and 64-bit platforms.

Cause

This problem occurs because during a small time frame, key presses may cause a part of Windows initialization to fail.

This problem does not cause any corruption or data loss, and the ntoskrnl.exe file is not corrupt as the error message says.

Workaround

To work around this issue, do not press any keys during startup until the Windows startup screen is displayed.

Windows doesn't start after you exclude UWF from Microsoft Defender

Article • 05/06/2022 • 2 minutes to read

This article discusses how to work around an issue in which Windows doesn't start after you exclude Unified Write Filter (UWF) from Microsoft Defender.

Applies to: Windows 10 Enterprise, Windows 10 IoT Enterprise or Windows 11 Enterprise

Issue

Consider the following scenario:

- You enable the UWF feature on a Windows 11 Enterprise-based, Windows 10 Enterprise-based, or Windows 10 IoT Enterprise-based computer.
- You configure a UWF registry exclusion for Windows Defender. Specifically, the following registry key is excluded from the write filter: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WdFilter`

In this scenario, the computer stops responding during Windows startup.

> **Note**
>
> - If you disable the UWF feature by using the `uwfmgr.exe filter disable` command, the issue doesn't occur.
> - The computer might start up after several retries.

This behavior is by design. To work around this issue, use an alternative menthod to exclude UWF.

Supported method to exclude UWF

To work around this issue, you can use the `Registry Commit` option for Uwfmgr.exe to exclude UWF. This option can commit changes to specify a value.

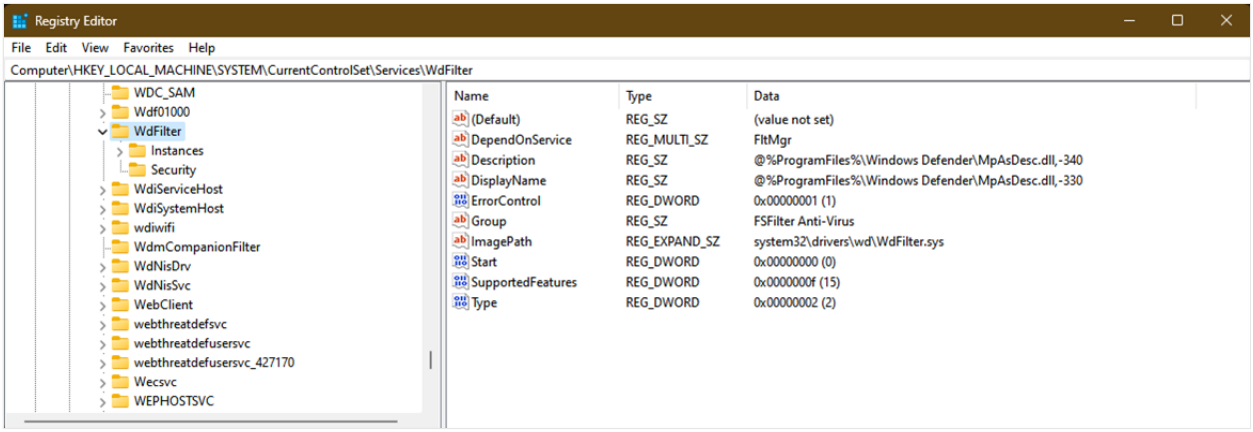
The following command can commit changes of a specified registry value:

```
Console
```

```
uwfmgr.exe registry commit "HKLM\SYSTEM\CurrentControlSet\Services\WdFilter"
Start
```

> **Note**
>
> Because the command can specify only a single registry value, you must specify the whole registry value for the registry keys where you want to commit changes.

For example, you find registry values that resemble the values in the following screenshot.



To commit all the changes that are made under the `WDFilter` registry subkeys, you have to run the `Registry Commit` option, as follows:

Console

```
uwfmgr.exe registry commit "HKLM\SYSTEM\CurrentControlSet\Services\WdFilter"
DependOnService
uwfmgr.exe registry commit "HKLM\SYSTEM\CurrentControlSet\Services\WdFilter"
Description
uwfmgr.exe registry commit "HKLM\SYSTEM\CurrentControlSet\Services\WdFilter"
DisplayName
uwfmgr.exe registry commit "HKLM\SYSTEM\CurrentControlSet\Services\WdFilter"
ErrorControl
uwfmgr.exe registry commit "HKLM\SYSTEM\CurrentControlSet\Services\WdFilter"
Group
uwfmgr.exe registry commit "HKLM\SYSTEM\CurrentControlSet\Services\WdFilter"
ImagePath
uwfmgr.exe registry commit "HKLM\SYSTEM\CurrentControlSet\Services\WdFilter"
Start
uwfmgr.exe registry commit "HKLM\SYSTEM\CurrentControlSet\Services\WdFilter"
SupportedFeatures
uwfmgr.exe registry commit "HKLM\SYSTEM\CurrentControlSet\Services\WdFilter"
Type
uwfmgr.exe registry commit
"HKLM\SYSTEM\CurrentControlSet\Services\WdFilter\Instances" DefaultInstance
uwfmgr.exe registry commit
```

```
"HKLM\SYSTEM\CurrentControlSet\Services\WdFilter\Instances\WdFilter
Instance" Altitude
uwfmgr.exe registry commit
"HKLM\SYSTEM\CurrentControlSet\Services\WdFilter\Instances\WdFilter
Instance" Flags
uwfmgr.exe registry commit
"HKLM\SYSTEM\CurrentControlSet\Services\WdFilter\Security" Security
```

> **Note**
>
> The Registry Commit option is a one-shot operation. It doesn't continue to bypass the write filter by running a single command. To make value changes commit whenever your computer shuts down, you must add this command set to the shutdown script.

For more inform about the shutdown script, see Working with startup, shutdown, logon, and logoff scripts using the Local Group Policy Editor.

More information

To check whether WDFilter registry keys are excluded from the UWF registry filter, open a Command Prompt window as an administrator, and then run `uwfmgr.exe get-config` at the prompt.

You cannot modify user environment variables in the System Properties dialog box if you log on by using a standard user account

Article • 12/06/2021 • 2 minutes to read

This article provides a resolution for the issue that you can't modify user environment variables in the System Properties dialog box.

Applies to: Windows Vista
Original KB number: 931715

Symptoms

If you log on by using a standard user account in Windows Vista, you can't modify user environment variables in the **System Properties** dialog box.

For example, if you try to access the System Properties dialog box by clicking **Advanced system settings** in the System item in Control Panel, you are prompted for administrator account credentials. If you type the credentials for an administrator account, the user environment variables that you can access are for that administrator account only.

Cause

This issue occurs because of increased security in Windows Vista. The method that you must use to modify user environment variables in Windows Vista differs from earlier versions of Microsoft Windows.

Resolution

To resolve this issue, modify the user environment variables by using the User Accounts item in Control Panel. You can follow these steps:

1. Click **Start**  , type Accounts in the **Start search** box, and then click **User Accounts** under **Programs**.

    If you are prompted for an administrator password or for a confirmation, type the password, or click **Allow**.

2. In the **User Accounts** dialog box, click **Change my environment variables** under **Tasks**.

3. Make the changes that you want to the user environment variables for your user account, and then click **OK**.

CPU usage exceeds 100% in Task Manager and Performance Monitor if Intel Turbo Boost is active

Article • 07/04/2022 • 2 minutes to read

This article describes an issue where CPU usage exceeds 100% in Task Manager and Performance Monitor if Intel Turbo Boost is active.

Applies to: Windows 8
Original KB number: 3200459

Symptoms

Starting with Windows 8, a change was made to the way that Task Manager and Performance Monitor report CPU utilization. With this change, CPU utilization may appear to exceed 100% when the system is under a heavy load, especially when capacity is boosted by Intel Turbo Boost.

Cause

This change affects the way that CPU utilization is computed. The values in Task Manager now correspond to the **Processor Information% Processor Utility** and **Processor Information% Privileged Utility** performance counters, *not* to the **Processor Information% Processor Time** and **Processor Information% Privileged Time** counters as in Windows 7.

More information

The difference between the two counter types concerns how they measure the actual work that the processor performs. The time-based performance counters measure the percentage of time that the processor is busy, whereas the utility performance counters measure how much work the processor actually performs. The utility performance counters take into account the processor performance state and Turbo Boost-based enhancements to measure and normalize the work that's being done by the CPU.

This change was intended to provide a more accurate representation of how much work the system is handling. A processor that's running 100% of the time and clocked down to 50% frequency performs only half the work of a processor that's running 100% of the

time at 100% frequency. Before this change, under the time-based performance counters (used in Windows 7 Task Manager), both processors appear to be doing the same amount of work: 100% of their capacity. With the redesigned Task Manager, the first processor is shown to be running at 50% capacity, whereas the second processor is shown to be running at 100% capacity. And Turbo Boost drives the processor above 100% of its nominal speed, and allows the processor to exceed 100% capacity.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

How to determine that hardware DEP is available and configured on your computer

Article • 03/24/2022 • 4 minutes to read

This article describes how to determine that hardware DEP is available and configured on your computer.

Applies to: Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 912923

Introduction

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help protect against malicious code exploits.

Hardware-enforced DEP marks all memory locations in a process as non-executable unless the location explicitly contains executable code. A type of malicious code attacks tries to insert and run code from non-executable memory locations. DEP helps prevent these attacks by intercepting them and raising an exception.

This article describes the requirements for using hardware-enforced DEP. This article also describes how to confirm that hardware DEP is working in Windows.

More information

Requirements for using hardware-enforced DEP

To use hardware-enforced DEP, you must meet all the following conditions:

1. The computer's processor must support hardware-enforced DEP.

   Many recent processors support hardware-enforced DEP. Both Advanced Micro Devices (AMD) and Intel Corporation have defined and shipped Windows-compatible architectures that are compatible with DEP. This processor support may be known as NX (no-execute) or XD (execute disable) technology. To determine whether your computer's processor supports hardware-enforced DEP, contact the manufacturer of your computer.

2. Hardware-enforced DEP must be enabled in the BIOS.

   On some computers, you can disable processor support for hardware-enforced DEP in the BIOS. This support can't be disabled. Depending on your computer manufacturer, the option to disable this support may be labeled "Data Execution Prevention," "XD," "Execute Disable," or "NX."

3. The computer must have Windows XP with Service Pack 2 or Windows Server 2003 with Service Pack 1 installed.

   > **Note**
   >
   > Both 32-bit versions and 64-bit versions of Windows support hardware-enforced DEP. Windows XP Media Center Edition 2005 and Microsoft Windows XP Tablet PC Edition 2005 include all the features and components of Windows XP SP2.

4. Hardware-enforced DEP must be enabled for programs on the computer.

   In 64-bit versions of Windows, hardware-enforced DEP is always enabled for 64-bit native programs. However, depending on your configuration, hardware-enforced DEP may be disabled for 32-bit programs.

For information about how to configure memory protection in Windows XP with Service Pack 2, visit the following Microsoft Web site:
https://technet.microsoft.com/library/cc700810.aspx

How to confirm that hardware DEP is working in Windows

To confirm that hardware DEP is working in Windows, use one of the following methods.

Method 1: Use the `Wmic` command-line tool

You can use the `Wmic` command-line tool to examine the DEP settings. To determine whether hardware-enforced DEP is available, follow these steps:

1. Click **Start**, click **Run**, type cmd in the **Open** box, and then click **OK**.
2. At the command prompt, type the following command, and then press ENTER:

```
Console
```

```
wmic OS Get DataExecutionPrevention_Available
```

If the output is "TRUE," hardware-enforced DEP is available.

To determine the current DEP support policy, follow these steps.

1. Click **Start**, click **Run**, type cmd in the **Open** box, and then click **OK**.
2. At the command prompt, type the following command, and then press ENTER:

   Console

   ```
   wmic OS Get DataExecutionPrevention_SupportPolicy
   ```

   The value returned will be 0, 1, 2 or 3. This value corresponds to one of the DEP support policies that are described in the following table.

DataExecutionPrevention_SupportPolicy property value	Policy Level	Description
2	OptIn (default configuration)	Only Windows system components and services have DEP applied
3	OptOut	DEP is enabled for all processes. Administrators can manually create a list of specific applications that do not have DEP applied
1	AlwaysOn	DEP is enabled for all processes
0	AlwaysOff	DEP is not enabled for any processes

> **Note**
>
> To verify that Windows is running with hardware DEP enabled, examine the DataExecutionPrevention_Drivers property of the Win32_OperatingSystem class. In some system configurations, hardware DEP may be disabled by using the /nopae or /execute switches in the Boot.ini file. To examine this property, type the following command at a command prompt:
> wmic OS Get DataExecutionPrevention_Drivers

Method 2: Use the graphical user interface

To use the graphical user interface to determine whether DEP is available, follow these steps:

1. Click **Start**, click **Run**, type `wbemtest` in the **Open** box, and then click **OK**.
2. In the **Windows Management Instrumentation Tester** dialog box, click **Connect**.
3. In the box at the top of the **Connect** dialog box, type root\cimv2, and then click **Connect**.
4. Click **Enum Instances**.
5. In the **Class Info** dialog box, type Win32_OperatingSystem in the **Enter superclass name** box, and then click **OK**.
6. In the **Query Result** dialog box, double-click the top item.

   > ⓘ Note
   >
   > This item starts with "Win32_OperatingSystem.Name=Microsoft..."

7. In the **Object editor** dialog box, locate the DataExecutionPrevention_Available property in the **Properties** area.
8. Double-click **DataExecutionPrevention_Available**.
9. In the **Property Editor** dialog box, note the value in the **Value** box.
   If the value is TRUE, hardware DEP is available.

> ⓘ Note
>
> - To determine the mode in which DEP is running, examine the DataExecutionPrevention_SupportPolicy property of the Win32_OperatingSystem class. The table at the end of Method 1 describes each support policy value.
> - To verify that hardware DEP is enabled in Windows, examine the DataExecutionPrevention_Drivers property of the Win32_OperatingSystem class. In some system configurations, hardware DEP may be disabled by using the /nopae or /execute switches in the Boot.ini file.

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, regarding the performance or reliability of these products.

GPU process memory counters report incorrect values

Article • 09/23/2021 • 2 minutes to read

This article discusses an issue where Graphics Processing Unit (GPU) process memory counters show memory leaks for running applications and report incorrect values.

Applies to: Windows 10 - all editions
Original KB number: 4490156

Symptoms

Graphics Processing Unit (GPU) process memory counters appear to show memory leaks for running applications in Windows 10, version 1709 and later. This issue affects the following counters:

- Performance Monitor: **GPU Process Memory**
- Task Manager, **Details** pane: **Dedicated GPU memory**

> ⓘ **Note**
>
> Some GPUs do not use dedicated GPU memory. In those cases, the **Dedicated GPU memory** counter is either not available or has a value of "0." The issue that this article describes does not occur.

Steps to reproduce the issue

> ⓘ **Note**
>
> Theses steps use an Office application as an example.

1. Right-click the Task bar, and then select **Task Manager**.
2. In Task Manager, select **Details**. On the **Details** pane, right-click a column head, select **Show columns**, and then select **Dedicated GPU memory**.
3. Start any Office application, create a blank document, and then maximize the application window.

4. Start any other application, and then maximize that application window in the same monitor as the Office application (so that the new application hides the Office application).

5. Wait approximately 30 seconds for the Office application to enter "Low Resource Mode."

   > ⓘ **Note**
   >
   > In this mode, the Office application flushes its discardable caches, including the GPU resources.

6. On the Task Manager **Details** pane, check the **Dedicated GPU memory** value for the Office application. You should notice that the value has dropped by approximately 100MB.

7. Bring the Office application window back to the monitor foreground.

   - **Expected behavior:** As the Office application re-creates its resources, its **Dedicated GPU memory** value should return to approximately the same value that it had the last time that the application was active.
   - **Actual behavior:** On systems that are affected by this issue, the new **Dedicated GPU memory** value is larger by approximately 100MB (or more) than the last time that the application was active. Every time that you hide the Office application, wait for it to flush its caches, and then reactivate it, the value increases by another 100MB (or more). However, the **Dedicated GPU memory** value that is visible on the Task Manager **Performance** pane continues to show the expected value. Additionally, tools such as Windows Performance Recorder (WPR) and Windows Performance Analyzer (WPA) show the expected value.

More information

This is a known issue in Windows 10. To monitor dedicated GPU memory on affected systems, use the **Performance** pane of Task Manager, WPR, or WPA. For more information about the GPU process memory counters, see GPUs in the Task Manager. For more information about WPR and WPA, see Windows Performance Toolkit.

Windows Task Manager shows incorrect CPU speed when Hyper-V is enabled

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where Windows Task Manager shows incorrect CPU speed when Hyper-V is enabled.

Applies to: Windows 10 - all editions, Window Server 2012 R2
Original KB number: 3003081

Symptoms

If the Hyper-V role is enabled in any of the products that are listed at the beginning of this article, the **CPU Frequency** speed value that is displayed in Task Manager is not the current speed, as expected. When the Hyper-V Role is not enabled, Task Manager correctly displays the current speed for this value.

Workaround

To work around this issue, use the built-in Performance Monitor tool (perfmon.exe), and add the "\Hyper-V Hypervisor Logical Processor\Frequency" performance counter.

Status

This is a known issue in the product versions that are listed at the beginning of this article.

User-defined data collector set doesn't run as scheduled

Article • 12/09/2021 • 2 minutes to read

This article provides a workaround for an issue in which a user-defined data collector set that is configured to run on a schedule does not run.

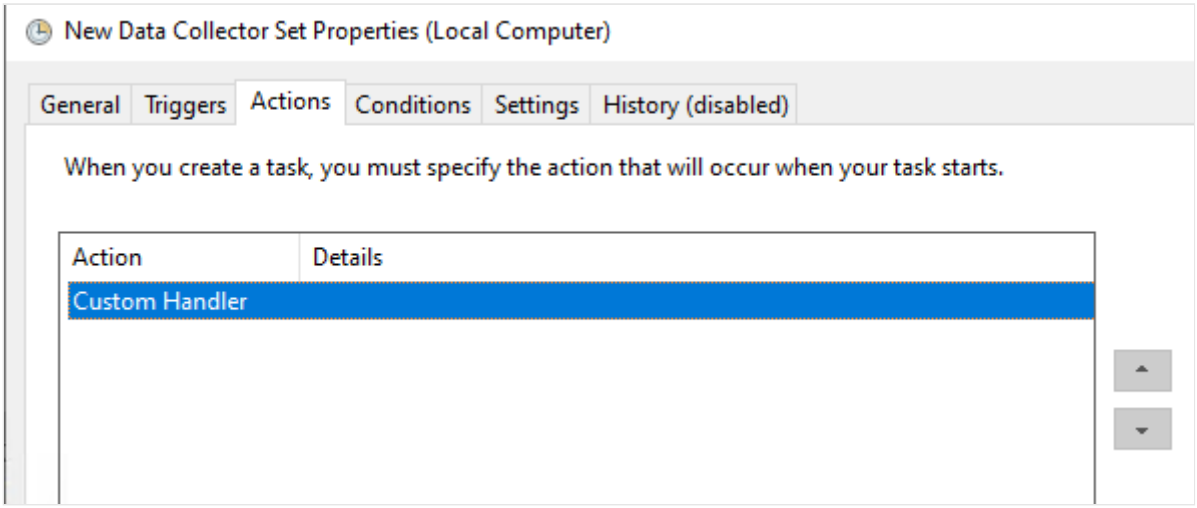
Applies to: Windows Server 2019 - all editions, Windows 10 version 1909 - all editions, Windows 10 version 1903 - all editions, Windows 10 version 1809 - all editions, Windows 10 version 1803 - all editions, Windows 10 version 1709 - all editions, Windows 10 version 1703 - all editions

Symptoms

In the Computer Management console in one of the affected versions of Windows, you create a data collector set in the **Performance** > **Data Collector Sets** > **User Defined** folder. You configure a schedule as part of the data collector set definition.

During the scheduled running time, you notice that Performance Monitor does not start collecting data. If you configured the data collector set to save data to a file, the file isn't created and no data is saved. In Task Scheduler, the task history indicates that the task ran successfully. However, the task didn't actually do anything.

In Task Scheduler, if you open the scheduled task and then select **Actions**, the actions list contains **Custom Handler**.



The list doesn't contain the expected action, **Start a program**, which includes the specific commands and arguments.

> **Note**
>
> In the Task Scheduler Library, tasks for data collector sets appear by default in **Microsoft** > **Windows** > **PLA**.

Cause

Starting in Windows 10 version 1703 and Windows Server 1703, the way that scheduled tasks are automatically created for data collector sets was changed. Because of the change, the actions for these tasks aren't created correctly.

Resolution

This issue is fixed in Windows 10, version 2004 and later versions and in Windows Server, version 2004 and later versions.

Workaround

You can manually fix the scheduled task that is associated with a data collector set. To do this, follow these steps:

1. In Task Scheduler, do one of the following to open the Properties dialog box of the affected task:
   - If the task appears in the **Active tasks** list in Task Scheduler, double-click the task. Then in the detailed task list, right-click the task and select **Properties**.
   - Go to **Task Scheduler Library** > **Microsoft** > **Windows** > **PLA**, right-click the task, and then select **Properties**.
2. Select **Actions**, select **Custom Handler**, and then select **Delete**.
3. Select **New**.
4. In **Program/script**, type the following string:

   ```
   cmd
   ```

   ```
   C:\windows\system32\rundll32.exe
   ```

5. In **Add arguments**, type the following string:

cmd

```
C:\windows\system32\pla.dll,PlaHost "{Name}" "$(Arg0)"
```

> **Note**
>
> In this string, {*Name*} represents the name of the data collector set.

6. Select **OK**.

How to use the System Configuration utility to troubleshoot configuration errors

Article • 12/06/2021 • 8 minutes to read

This article describes how to use the System Configuration utility to troubleshoot configuration errors.

Applies to: Windows Vista
Original KB number: 950093

Introduction

This article describes how to use the System Configuration utility (Msconfig.exe) to troubleshoot configuration errors that might prevent Windows Vista from starting correctly.

More information

The System Configuration utility finds and isolates issues. However, it is not a startup management program.

For more information about how to disable or to permanently remove the programs that run when Windows starts, click the following article number to view the article in the Microsoft Knowledge Base:

270035 How to disable programs that run when you start Windows XP Home Edition or Windows Vista

Advanced troubleshooting

These troubleshooting steps are intended for advanced computer users. If you are not comfortable with advanced troubleshooting, you might want to ask someone for help or to contact support. For information about how to contact support, visit the following Microsoft Web site:
Microsoft Support
The System Configuration utility automates the routine troubleshooting steps that

Microsoft Customer Support Services professionals use when they diagnose system configuration issues.

When you use this utility, you can select options to temporarily prevent services and programs from loading during the Windows startup process. With this process, you can reduce the risk of making typing errors when you use Registry Editor. Additionally, when you use the utility, it is easy to restore the original configuration.

When you use the System Configuration utility, you can start Windows while common services and startup programs are disabled. Then, you can enable them one at a time. If an issue does not occur when a service is disabled but does occur when the service is enabled, the service could be the cause of the issue.

You can easily reset or change the configuration settings in Windows Vista to include preferences for the following settings:

- Startup options
- Services that are set to start during the startup process
- Programs that are set to load during the startup process

> ⓘ **Note**
>
> These programs are specified in the Programs/Startup folders and in the registry.

> ⓘ **Note**
>
> To use the System Configuration utility, you must be logged on as an administrator or as a member of the Administrators group.

Startup options that are available

The following startup options are available:

- Normal startup
- Diagnostic startup
- Selective startup

Normal startup

The normal startup option is the Windows default. This option enables Windows to start in normal mode together with all programs, services, and device drivers loaded.

Diagnostic startup

The diagnostic startup option enables Windows to determine which basic device drivers and software to load when you start Windows. When you use this option, the system temporarily disables Microsoft services such as the following services:

- Networking
- "Plug and Play"
- Event Logging
- Error Reporting
- System Restore

> ⓘ **Note**
>
> Do not use this option if you have to use a Microsoft service to test an issue.

To perform a diagnostic startup, follow these steps:

1. Click **Start**  , type `msconfig` in the **Start Search** box, and then press ENTER.

    If you are prompted for an administrator password or for a confirmation, type the password, or click **Continue**.

2. On the **General** tab, click **Diagnostic startup**, and then click **OK**.

3. Click **Restart**.

If the issue does not occur after Windows restarts, use the selective startup option to try to find the issue by disabling and enabling individual services and startup programs.

Selective startup

The selective startup option enables you to select the programs and services that you want the computer to load when you restart the computer. You can select from the following options:

- **Load system services**
- **Load startup items**
- **Use original boot configuration**

By default, all these options are selected. The following rules apply to these options:

- When you click to select the check box, the option is processed when you restart the computer.
- When you click to clear the check box, the option is not processed when you restart the computer.
- When the check box is selected and when you cannot click to clear the check box because it is unavailable, some items are still loading from that option when you restart the computer.
- When the check box is not selected and when you cannot click to select the check box because it is unavailable, the option is not present on the computer.
- You cannot change the **Use original boot configuration** option.

> ⓘ **Note**
>
> When you click to clear the **Load system services** check box, you disable Microsoft services such as the following services:
>
> - Networking
> - "Plug and Play"
> - Event Logging
> - Error Reporting
> - System Restore

Do not click to clear this check box if you have to use a Microsoft service to test an issue.

To perform a selective startup and to troubleshoot the issue, follow these steps:

1. Click **Start**  , type `msconfig` in the **Start Search** box, and then press ENTER.

    If you are prompted for an administrator password or for a confirmation, type the password, or click **Continue**.

2. On the **General** tab, click **Selective startup**, and then click to clear the **Load system services** and **Load startup items** check boxes.

3. Click **OK**, and then click **Restart**.

If you can reproduce the issue after the computer restarts, the issue is not related to system services or startup items. In this case, the System Configuration utility will not help troubleshoot the issue.

If you cannot reproduce the issue after the computer restarts, the issue is related to either the system services or the startup items. To determine the items to which the issue is related, follow these steps:

1. Click **Start** , type `msconfig` in the **Start Search** box, and then press ENTER.

   If you are prompted for an administrator password or for a confirmation, type the password, or click **Continue**.

2. On the **General** tab, click **Selective startup**, and then click to select the **Load system services** check box.

3. Click **OK**, and then click **Restart**.

If you can reproduce the issue after the computer restarts, the issue is related to one of the system services. Otherwise, the issue is related to one of the startup items.

After you determine the items to which the issue is related, follow the steps in the "How to determine the service or startup item that is causing the issue" section to determine the individual service or startup item that is causing the issue.

How to determine the service or startup item that is causing the issue

To determine the cause of the issue, you can prevent individual services and startup items from loading when you restart the computer. You can follow these steps.

How to determine the system service that is causing the issue

1. Click the **Services** tab, click **Disable all**, click to select the check box for the first service that is listed, and then restart the computer.

   If the issue doesn't occur, you can eliminate the first service as the cause.

2. With the first service selected, click to select the check box for the second service, and then restart the computer.

3. Repeat this process until you reproduce the issue. If you cannot reproduce the issue, you can eliminate system services as the cause. Continue to the next procedure.

How to determine the startup item that is causing the issue

1. Click the **General** tab, and then click to select the **Load startup items** check box.
2. Click the **Startup** tab, click **Disable all**, click to select the check box for the first startup item that is listed, and then restart the computer.

   If the issue does not occur, you can eliminate the first startup item as the cause.
3. With the first startup item selected, click to select the check box for the second startup item, and then restart the computer.
4. Repeat this process until you reproduce the issue.

How to enable and to disable individual services and startup items

Services and startup options

The **Services** and **Startup** tabs in the System Configuration utility have the following options:

- Check boxes enable you to enable or to disable an option. To enable or to disable an option so that it loads or does not load at startup, click to select or click to clear the check box. A selected check box indicates that the option will be started or loaded at startup.
- The keyboard arrow keys enable you to move through the different options when you do not have a mouse.
- The SPACEBAR enables you to select and to clear options when you do not have a mouse.

> ⓘ **Note**
>
> When you click to clear a check box for an item, the **Selective Startup** option on the **General** tab is automatically selected.

How to return to normal startup

After you complete your troubleshooting and fix your configuration, return to a normal startup. You can follow these steps:

1. Click **Start**  , type `msconfig` in the **Start Search** box, and then press ENTER.

 If you are prompted for an administrator password or for a confirmation, type the password, or click **Continue**.

2. On the **General** tab, click **Normal startup**, and then click **OK**.

3. Click **Restart**.

How to start diagnostic tools and other advanced tools

You can use the **Tools** tab in the System Configuration utility to start diagnostic tools and other advanced tools. The **Tools** tab also displays the path and the switches for the tools.

To start one or more of the tools that are listed on the **Tools** tab, click the tool that you want to start, and then click **Launch**. Or, click the tool that you want to start, and then press ALT+L.

References

For more information about advanced troubleshooting for general startup problems in Windows Vista, click the following article number to view the article in the Microsoft Knowledge Base:

927392 How to use the Bootrec.exe tool in the Windows Recovery Environment to troubleshoot and repair startup issues in Windows Vista

For more information about how to use System Restore to restore Windows Vista, click the following article number to view the article in the Microsoft Knowledge Base:

936212 How to repair the operating system and how to restore the operating system configuration to an earlier point in time in Windows Vista

For more information about how to configure Windows Vista to start in a "clean boot" state, click the following article number to view the article in the Microsoft Knowledge Base:

929135 How to troubleshoot a problem by performing a clean boot in Windows Vista

If these articles can't help you resolve the issue or if you experience symptoms that differ from those ones described in this article, search the Microsoft Knowledge Base for more information. To search the Microsoft Knowledge Base, visit the following Microsoft Web site:
https://support.microsoft.com

Type the text of the error message that you receive, or type a description of the issue in the **Search** box, and then press ENTER.

Windows Experience Index shows "1.0" for graphics subscore

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where WinSAT fails to generate the correct Windows Experience Index score when you build an image for Windows 7 deployment.

Applies to: Windows 7 Service Pack 1
Original KB number: 2716476

Symptoms

Consider the following scenario:

- You're building an image for Windows 7 deployment. All supplemental components are also installed.
- You run the WinSAT prepop command to generate a Windows Experience Index score.
- You run sysprep to seal the image for deployment.

After the Out of Box Experience (OOBE) phase, you may find the Windows Experience Index score is "1.0", and you also find the Graphics Subscore is "1.0".

If you go to C:\Windows\Performance\WinSAT\DataStore folder and check the file named DWM.Assessment (Prepop).WinSAT.xml, you may find the following sentence logged into the file:

XML

```
<LimitsApplied>
    <GraphicsScore>
        <LimitApplied Friendly="Limiting DWM Score to 1.0 - no DWM
performance score">NoScore</LimitApplied>
    </GraphicsScore>
</LimitsApplied>
```

Cause

Windows 7 introduced the Diagnostics Performance kernel component (PerfTrack), which wasn't included in earlier versions of Windows. Due to some timing factors, PerfTrack may occasionally stop the Circular Kernel Context Logger (CKCL) while WinSAT

is using it for a performance assessment. If this happens, WinSAT will fail to generate the correct score and will return a score of 1.0 for the assessment.

Resolution

If you rerun the Windows Assessment (WinSAT), the graphics score should be calculated correctly.

If you are a system builder or OEM and you frequently encounter this issue, consider the following steps to work around the problem:

1. Add the following commands to a batch file and run the batch in WinPE against the image:

   ```
   Console

   reg load HKLM\TempHiv %WinDRV%\Windows\system32\config\system
   reg add HKLM\TempHiv\ControlSet001\Control\Diagnostics\Performance /v
   DisableDiagnosticTracing /t REG_DWORD /d 1 /f
   reg unload HKLM\TempHiv
   ```

2. Reboot, then run WINSAT prepop.

3. Run sysprep tool.

4. Restart the system in WinPE and then run the following commands:

   ```
   Console

   reg load HKLM\TempHiv %WinDRV%\Windows\system32\config\system
   reg add HKLM\TempHiv\ControlSet001\Control\Diagnostics\Performance /v
   DisableDiagnosticTracing /t REG_DWORD /d 0/f
   reg unload HKLM\TempHiv
   ```

More information

Configure Windows System Assessment Tests Scores

Push-button reset fails because language resources are missing

Article • 09/02/2022 • 2 minutes to read

This article describes an issue in which push-button reset fails because language resources are missing, and provides a workaround for the issue.

Applies to: Windows 10 Education, version 2004

Symptoms

Push-button reset (PBR) fails and a user receives the error message, **There was a problem resetting your PC. ErrorCode 0x80041002, WBEM_E_NOT_FOUND**.

The issue occurs after leaving a personal computer (PC) idle, and a PBR Reset command is executed. This issue may also occur after executing a **SilentCleanup** task. The issue is seen PCs with multiple language resources.

Cause

This error is a known issue. If PBR fails in an early stage and rollback, the rollback process will set the Windows Recovery Environment (WinRE) Boot Configuration Data (BCD) as the default BCD entry, but will fail to restore the default BCD entry to the Operating System (OS). Changing the default BCD entry to the WinRE entry will cause a successful PBR to delete the WinRE entry, and disable the WinRE BCD.

The following steps reproduce this error:

1. Set up a PC without including language resource 2020.8B.
2. Execute SilentCleanupTask manually.
3. Apply language resource 2020.8B to the PC.
4. Execute PBR Reset/Refresh. PBR fails with the error message, **There was a problem resetting your PC**.

This issue will be resolved in next Windows OS upgrade release.

Resolution

Workaround for users with internet

For users who can access internet:

When the issue is reproduced, WinRE is installed correctly, but its BCD entry is accidentally deleted. To correct this issue, run the `Reagentc /enable` command twice from an administrator command prompt.

When the first `Reagentc /enable` runs, it will ask about the state of the WinRE, and it will detect the current WinRE state. Although `Reagentc /enable` cannot fix the issue, it will perform a cleanup, and will fully uninstall the WinRE. The WinRE file still exists (copied to staging location) allowing it to be enabled in the future.

When the second `Reagentc /enable` runs, the WinRE file is purged. It can then be installed for the OS, and run without issue.

> ⓘ **Note**
>
> When `Reagentc /enable` runs for the first time, it will report the error message, **Unable to update Boot Configuration Data**.
>
> When `Reagentc /enable` runs for the second time, WinRE will be enabled.

Workaround for users without internet access

For users who can't access internet:

1. Apply language resource 2020.8B.
2. Run `Dism /online /cleanup-image /restorehealth`.
3. Run **PBR Reset/Refresh**.
4. Attempt a PBR.
5. Rerun **PBR Reset/Refresh**.
6. Run `reagentc /enable` twice.
7. Run the **PBR Reset/Refresh**.

> ⓘ **Note**
>
> There is a scenario that is currently under investigation where the `Reagentc /enable` will not fix the issue previously discussed. If the staging location is same as the location of the WinRE, the current logic of `Reagentc /enable` will not work.

Microsoft is updating the logic in `Reagentc /enable`, and will release the updated command as part of a Latest Cumulative Update (LCU).

More information

- Push-button reset
- How Push-button reset works
- Windows Recovery Environment (Windows RE)

Windows shuts down slowly when it is set to clear the virtual memory pagefile on shutdown

Article • 09/23/2021 • 2 minutes to read

This article provides a solution for the issue Windows shuts down slowly when it is set to clear the virtual memory pagefile on shutdown.

Applies to: Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 320423

Symptoms

When the Clear virtual memory pagefile when system shuts down Group Policy setting is turned on in Windows Server 2003 and in later versions, the computer may take longer to shut down than it usually takes. This setting is called Shutdown: Clear virtual memory pagefile in Windows Vista and later versions.

Cause

This behavior occurs because when this policy setting is turned on, the computer must physically write to each page in the pagefile to clear each page. The period of time that it takes for the system to clear the pagefile varies according to the pagefile size, and the disk hardware that is involved.

Status

This behavior is by design.

> **Note**
>
> This issue also occurs when the Group Policy setting is turned on in Windows XP and in Windows Server 2003.

More information

By default, the Clear virtual memory pagefile when system shuts down Group Policy setting is turned off. To confirm this setting on Windows 2000, on Windows XP, or on Windows Server 2003, follow these steps:

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Administrative Tools**.
3. Double-click **Local Security Policy**.
4. Double-click **Local Policies**.
5. Click **Security Options**.
6. Look in the **Effective Setting** column to the right side of the Clear virtual memory pagefile when system shuts down entry.

To check this setting on Windows Vista and on later versions, follow these steps:

1. Click **Start**, type secpol.msc, and then press ENTER.
2. Expand **Local Policies**.
3. Click **Security Options**.
4. Look in the '**Security Setting** column to the right side of the Shutdown: Clear virtual memory pagefile entry.

High CPU usage in the LSAISO process on Windows

Article • 12/06/2021 • 3 minutes to read

This article provides resolutions of a problem in which the LSAISO process experiences high CPU usage on a computer that's running Windows.

Applies to: Windows 10 - all editions, Windows Server 2016, Windows Server 2019
Original KB number: 4032786

Symptoms

The LSAISO (LSA Isolated) process experiences high CPU usage on a computer that's running Windows 10, Windows Server 2016, or later versions.

Cause

In Windows, the LSAISO process runs as an Isolated User Mode (IUM) process in a new security environment that is known as Virtual Secure Mode (VSM).

Applications and drivers that try to load a DLL into an IUM process, inject a thread, or deliver a user-mode APC may destabilize the entire system. This destabilization can include the high LSAISO CPU scenario that is mentioned in the "Symptoms" section.

Resolution 1: Use the process of elimination

It's common for some applications (such as antivirus programs) to inject DLLs or queue APCs to the LSAISO process. This causes the LSAISO process to experience high CPU usage.

For troubleshooting, it's not possible to attach tools to a IUM process. This prevents you from using the Windows Debugging Tools or WPA\XPERF to capture stack traces during the LSAISO CPU spiking. So the best troubleshooting method in this scenario is to use the "process of elimination" methodology. To do this, disable applications and drivers until the CPU spike is mitigated. After you determine which software is causing the problem, contact the vendor for a software update. You can reference the ISV recommendations that are listed in the following MSDN topic:

Isolated User Mode (IUM) Processes

> ⓘ Note
>
> This method may require a reboot after you disable the suspected software and drivers as you test for the CPU spike.

Resolution 2: Check for queued APCs

Download the free Debugging Tools for Windows (WinDbg, KD, CDB, NTSD). These tools are included in both the Windows Driver Kit (WDK) and the Windows Driver Kit (WDK). Then, follow these steps to determine which driver is queuing an APC to LSAISO:

1. While you reproduce the CPU spike, generate a kernel memory dump by using a tool such as NotMyFault.exe from the following Sysinternals website:

   Sysinternals Suite

   > ⓘ Note
   >
   > A complete memory dump isn't recommended because it would require decryption if VSM is enabled on the system. To enable the kernel dump, follow these steps:

   a. Open the **System** item in Control Panel, and then select **Advanced system settings**.
   b. On the **Advanced** tab of the **System Properties** dialog box, select **Settings** in the **Startup and Recovery** area.
   c. In the **Startup and Recovery** dialog box, select **Kernel memory dump** in the **Write debugging information** list.
   d. Note the **Dump File** location to use in step 5, and then select **OK**.

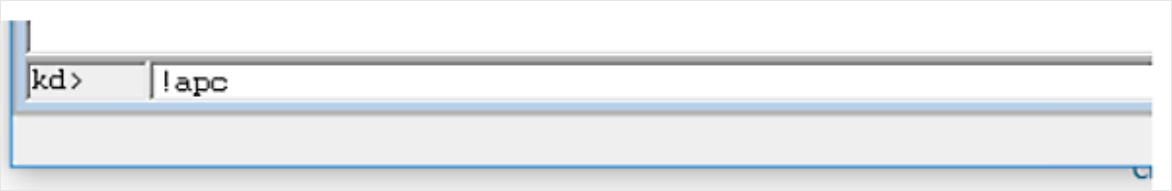
2. Open the WinDbg.exe tool from the Debugging Tools for Windows.

3. On the **File** menu, click **Symbol File Path**, add the following path for the Microsoft Symbol Server to the **Symbol path** box, and then select **OK**:
   `https://msdl.microsoft.com/download/symbols`

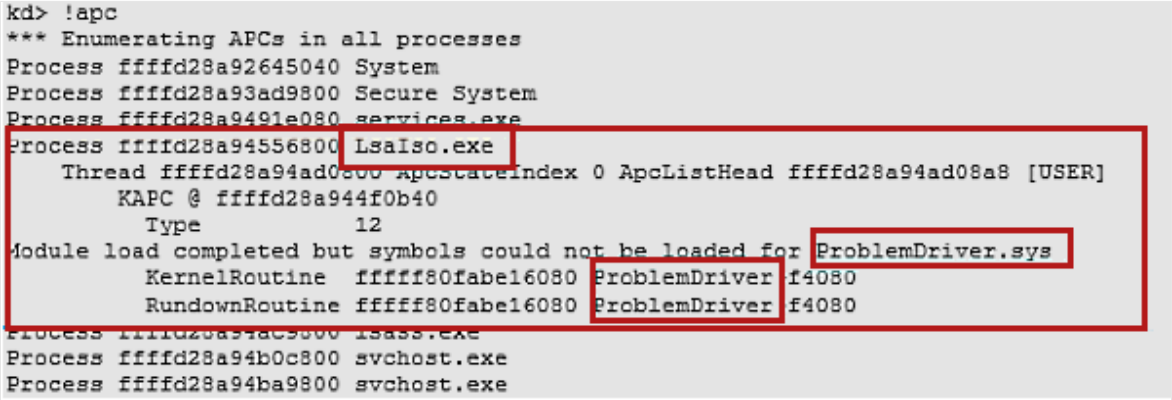
4. On the **File** menu, click **Open Crash Dump**.

5. Browse to the location of the kernel dump file that you noted in step 1d, and then select **Open**. Check the date on the .dmp file to make sure that it was newly created during this troubleshooting session.

6. In the **Command** window, type **!apc**, and then press Enter.



The output should resemble the following screenshot.



7. Search the results for **LsaIso.exe**. If a driver that is named <ProblemDriver>.sys is listed under **LsaIso.exe** (as shown in the example screenshot of output in step 6), contact the vendor, and then refer them to the recommended mitigation that is listed in the Isolated User Mode (IUM) Processes topic.

> ⓘ **Note**
>
> If no drivers are listed under **Lsaiso.exe**, this means that the LSAISO process has no queued APCs.

More information

VSM uses isolation modes that are known as Virtual Trust Levels (VTL) to protect IUM processes (also known as trustlets). IUM processes such as LSAISO run in VTL1 while other processes run in VTL0. The memory pages of processes that run in VTL1 are protected from any malicious code that is running in VTL0.

Prior to Windows 10 and Windows Server 2016, the Local Security Authority Subsystem Service (LSASS) process was solely responsible for managing the local system policy, user authentication, and auditing while it also handled sensitive security data such as password hashes and Kerberos keys.

To use the security benefits of VSM, the LSAISO trustlet that runs in VTL1 communicates through an RPC channel with the LSAISO process that's running in VTL0. The LSAISO

secrets are encrypted before they're sent to LSASS, and the pages of LSAISO are protected from any malicious code that's running in VTL0.

Speed up a Windows 8.1 computer

Article • 09/23/2021 • 10 minutes to read

No matter how good you are about keeping your computer clean and up-to-date, they tend to slow down after time. Fortunately, there are a lot of ways to help speed them up— without upgrading your hardware.

Applies to: Windows 8.1
Original KB number: 3064207

> ⓘ **Note**
>
> If you are an advanced user, you can download **a free tool** from the Microsoft website that shows you all of the programs and processes that run when you start Windows, including the ones that Windows requires to operate successfully. Use this tool only if you are comfortable restoring Windows after an error occurs.

Uninstall extra antivirus programs

If you use more than one antivirus or antispyware program at the same time, your device may experience decreased performance, become unstable, or restart unexpectedly. To remedy the issue, you should select one Internet security program to run on your device. You should then uninstall the other programs.

> ⊗ **Caution**
>
> Make sure you have an Internet security program running on your device before you uninstall other security programs.

Some Internet security applications do not uninstall completely. You may need to download and run a cleanup utility for your previous security application to completely remove it.

If you use another antispyware program together with Microsoft Security Essentials, we recommend that you turn off real-time scanning in the other program. For more information, see the documentation supplied by that antispyware program.

To remove an antivirus or antispyware program, follow these instructions:

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or select **Search**.
3. Type *appwiz.cpl* in the **Search** box.
4. Tap or select **Appwiz.cpl** below the **Search** box.
5. In the list of installed programs, uninstall the Internet security programs you don't need.
6. Restart your device.

Close programs in the notification area running with startup

If your device takes a long time to start up, one of the causes could be having a large number of startup apps or a few apps that have a high impact on startup time.

Some of these programs add an icon to the notification area on the taskbar to show that they are running with startup.

To stop a program that has one of these icons from automatically running on startup, follow these instructions:

1. Point to each icon in the icon tray to see the program name.
2. To ensure that you can see icons for all running programs, swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down), and tap or select **Search**.
3. Type *show hidden icons* in the **Search** box.
4. Tap or select **Show or hide inactive icons on the taskbar**.
5. Check **Always show all icons and notifications on the taskbar**.

> ⓘ **Note**
>
> You must open any program that you do not want to run on startup and change the setting.

View Startup items

To see what programs run at startup and disable any, follow these instructions:

1. Press and hold or right-click in the blank area on Taskbar and select **Task Manager**.
2. Tap or select **More details** in the lower-left corner of **Task Manager**.

3. Under the **Startup** tab in **Task Manager**, you can view a list of applications that start automatically every time you turn on your device and sign in to Windows.
4. If you see any programs in this list that you do not want to run when Windows starts, tap or select the application and then tap or select **Disable**.

> **Note**
>
> Disabling a program from running at startup doesn't stop the program from running if you need it. If you tap or select the program after startup, it will start and run normally.

Change a program

Sometimes, by adding or removing certain program options, you can prevent a program from running at startup.

If you can't stop the program from running on startup and the program does not have the option to change the configuration, you must talk to the program manufacturer for a solution.

To change the configuration of a program, follow these instructions:

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or select **Search**.
3. Type *appwiz.cpl* in the **Search** box.
4. Tap or select **Appwiz.cpl** below the **Search** box.
5. Tap or select a program, and then tap or select **Uninstall**, **Change**, or **Repair**.

If prompted, type an administrator password or confirmation.

Clean up disk errors

Over time, your device may create errors on its hard drive. These errors can slow your device. The Check Disk program identifies and cleans any errors.

To run Check Disk, follow these instructions:

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).

2. Tap or select **Search**.

3. Type *computer* in the **Search** box.
4. Tap or select **This PC** below the **Search** box.
5. Press and hold or right-click the drive you want to repair, and then tap or select **Properties**.
6. Tap or select the **Tools** tab.
7. Under **Error checking**, tap or select **Check**. Depending upon the size of your hard disk, this may take several minutes. For best results, don't use your device for any other tasks while it's checking for errors. If prompted, type an administrator password or confirmation.
8. You may need to restart your device after error checking is complete.

Defragment your hard disk

One of the best ways to help improve your device's performance is by optimizing the hard drive. Optimize Drives, previously known as Disk Defragmenter, is a Windows feature that helps optimize different types of drives. The feature runs automatically on a weekly schedule, but you can also run Optimize Drives manually.

To run Optimize Drives manually, follow these instructions:

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or select **Search**.
3. Type *computer* in the **Search** box.
4. Tap or select **This PC** below the **Search** box.
5. Press and hold or right-click the drive you want to repair, and then tap or select **Properties**.
6. Tap or select the **Tools** tab.
7. Tap or select **Optimize** under **Optimize and defragment drive**.
8. Under **Status**, tap or select the drive you want to optimize. (The **Media type** column tells you what type of drive you're optimizing.)
9. To determine if the drive needs to be optimized, tap or select **Analyze**.

> ⓘ **Note**
>
> If prompted, type an administrator password or confirmation.

10. After Windows finishes analyzing the drive, check the **Current status** column to see whether you need to optimize the drive. If the drive is more than 10 percent fragmented, you should optimize it.
11. Tap or select **Optimize**.

> **Note**
>
> - Optimizing a drive can take anywhere from several minutes to several hours to finish, depending on the size of the drive and degree of optimization required. You can still use your device during the optimization process.
> - If the drive is being used by another program or is formatted using a file system other than NTFS, FAT, or FAT32, it can't be optimized.
> - Network drives can't be optimized.
> - If a drive doesn't appear in Optimize Drives, it might be because it contains an error. Try to repair the drive first, then return to Optimize Drives to try again.

To change the optimization schedule, follow these instructions:

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or select **Search**.
3. Type *computer* in the **Search** box.
4. Tap or select **This PC** below the **Search** box.
5. Press and hold or right-click the drive you want to repair, and then tap or select **Properties**.
6. Tap or select the **Tools** tab.
7. Tap or select **Optimize** under **Optimize and defragment drive**.
8. Tap or select **Change settings**. If prompted, type an administrator password or confirmation.
9. Select one of the following:
    - To turn off scheduled optimization, clear the **Run on a schedule** check box.
    - To change the frequency of scheduled optimization, tap or select the drop-down list next to **Frequency**, and then tap or select **Daily**, **Weekly**, or

Monthly. The default schedule for optimization is weekly and runs during Automatic Maintenance.

- To select the drives you want to include or exclude in scheduled optimization, tap or select **Choose** next to Drives. Select or clear the check boxes next to the drives and then tap or select OK. You can also clear the **Automatically optimize new drives** check box if you don't want new drives added to scheduled optimization. If Windows can't optimize a drive, it won't offer the drive as an option for Automatic Maintenance.

10. Tap or select **OK**.

Clean your hard disk

Disk Cleanup reduces the number of unnecessary files on your drives by deleting temporary files and system files, emptying the Recycle Bin, and removing a variety of other items that you may no longer need.

To clean your hard disk, follow these instructions:

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or select **Search**.
3. Type *free up disk space* in the **Search** box.
4. Tap or select **Free up disk space by deleting unnecessary files** below the **Search** box.
5. In the **Drives** list, tap or select the drive that you want to clean up.
6. Tap or select **OK**.
7. In the message that appears, tap or select **Delete files**.

To clean up system files associated with your account, follow these instructions:

1. In the **Drives** list, tap or select the drive that you want to clean up and then tap or select **OK**.
2. In the Disk Cleanup dialog box, tap or select **Clean up system files**.

   > ⓘ **Note**
   >
   > If prompted, type an administrator password or confirmation.

3. The **More Options** tab is available when you opt to clean up system files from your device. This tab includes two additional options for freeing up space:

- **Programs and Features**. This option opens **Programs and Features** in **Control Panel**, where you can uninstall programs that you no longer use. The **Size** column in **Programs and Features** shows how much space each program uses.
- **System Restore and Shadow Copies**. System Restore uses restore points to return your system files to an earlier point in time. If your device is running normally, you can save space by deleting earlier restore points.

Turn off visual effects

If Windows is running slowly, you can speed it up by disabling certain visual effects. You can select which visual effects to turn off one by one or you can let Windows select for you.

To turn off visual effects, follow these instructions:

1. Swipe in from the right edge of the screen (if using a mouse, point to the upper-right corner of the screen and move the mouse pointer down).
2. Tap or select **Search**.
3. Type *Performance Information and Tools* in the **Search** box.
4. Tap or select **Adjust the appearance and performance of Windows** below the **Search** box.
5. Under **Visual Effects** tab, check on **Adjust for best performance**, and then tap or select **OK**. (For a less drastic option, select **Let Windows choose what's best for my computer**.

Run fewer programs at the same time

Sometimes you can improve system performance by changing your computing behavior. Running four or more programs while leaving multiple browser windows and email messages open may be more than your device can handle.

If you find your device slowing down, decide whether you really need to keep all of your programs and windows open at the same time. Also, find a way to remind yourself to reply to email messages later instead of keeping them open until you reply.

Use ReadyBoost

ReadyBoost can speed up your device by using storage space on flash memory cards and USB flash drives. If you have a storage device that will work with ReadyBoost, you'll

see an option to use ReadyBoost when you plug it into your device. If you select this option, you can select how much memory to use.

Adjust indexing options

Windows uses an index to perform very fast searches of the most common files on your device. If it's taking too long to search for things on your device, you can narrow your search to focus on the files and folders that you most commonly use.

Adjust power plan

A power plan is a collection of hardware and system settings (such as display, sleep, and so on) that manages how your device uses power. The power plans you can use depend on the kind of device you have.

Memory leak in the remote registry service causes Windows to hang

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for a memory leak issue in the remote registry service that causes Windows to hang.

> **Note**
>
> This issue is fixed in Windows 10.

Applies to: Windows Server 2012 R2
Original KB number: 3105719

Symptoms

On a Windows-based computer, you notice that more system memory and paged pool memory are being consumed than expected. This memory leak occurs after about 10 minutes of system uptime and eventually causes the system to hang.

Additionally, PoolMon analysis may show that the Windows Notification Facility (WnF) tag is consuming all the available paged pool memory.

Cause

The issue occurs in the Endpoint Mapper Logic component. The Remote Registry service is designed to stop running after the connection has been idle for 10 minutes.

Workaround

To work around this issue, follow these steps:

1. Open the run command box by pressing the Windows key+R.
2. Type *regedit.exe*, and then press Enter.
3. Locate the following registry subkey:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RemoteRegistry`

4. In the details pane (on the right side), double-click **DisableIdleStop**.

5. Change the value to 00000001.

> **Note**
>
> The default value is 00000000.

6. Exit Registry Editor.

Troubleshooting slow file copying in Windows

Article • 12/06/2021 • 4 minutes to read

This article helps administrators to diagnose and resolve the issue of slow file copy in your organization.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 10118

Determine the cause of the issue

Slow file copying can be caused by storage issues, client issues, and server issues.

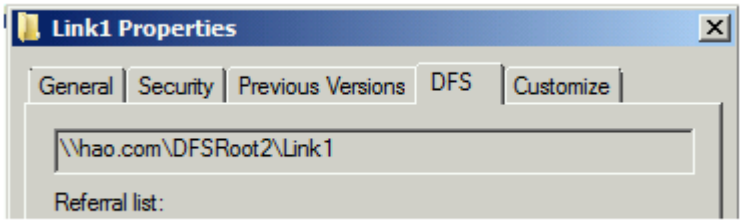
On the file server that hosts the shared folder, copy the file to its local hard disk. If the file-copying speed is unusually low (much slower than average speed), try to update the driver for your storage. If the issue still occurs, contact the driver manufacturer for further troubleshooting.

If the speed is normal, use another client computer to copy the files from or to the shared folder.

- If the file copy speed is still slow, see server-side troubleshooting.
- If issue doesn't occur, see client-side troubleshooting.

Client-side troubleshooting

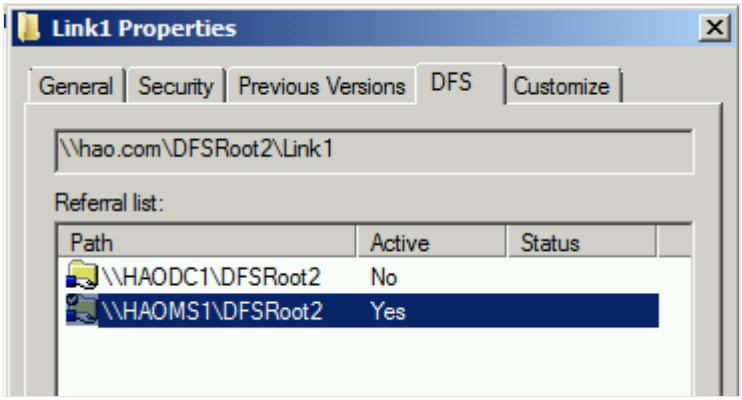
Let's verify the kind of the shared folder. To do so, open the properties of the shared folder. For the Distributed File System (DFS) shared folder, the **DFS** tab is displayed.



The share folder is a DFS shared folder

Let's determine whether the problem is caused by the DFS path. Try to use the UNC path instead of the DFS path to open the shared folder. Then, you can check whether the issue still occurs. This step can help you determine whether the problem is caused by the DFS path. How to determine the UNC path of the DFS shared folder:

1. Right-click the shared folder, and then select **Properties**.
2. On the **DFS** tab, you see the UNC path in **Referral list**.



If it is still slow when you use the UNC path, see slow performance when you copy a single file, a folder, or multiple files.

If the issue does not occur when you use the UNC path, follow these steps to verify the DFS referrals.

Verify the DFS referrals

1. Right-click the shared folder, and then select **Properties**. On the **DFS** tab, locate all active referrals.
2. Remove UNC paths that aren't active or servers that aren't reachable or are removed.
3. Connect these paths one by one, and make sure that all destination paths can be reached directly from the client. By design, if the client can't connect the first referral, it will switch to the second and so on. It will create a delay.

If the issue is still not resolved, see server side troubleshooting.

The share folder is not a DFS shared folder

Check when the slow file copying problem occurs.

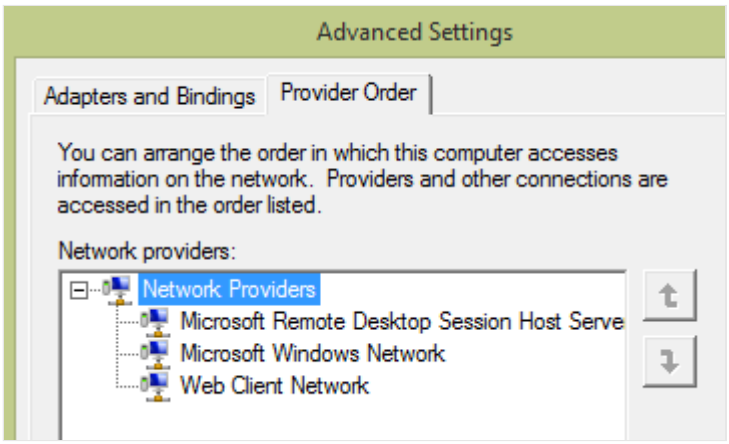
Slow performance occurs only when you copy a folder or multiple files

If you compare the copying time for a folder that contains multiple files with the copying time for a file of the same size, copying the folder will always require more time. This behavior is expected. The more files that are in the folder, the slower the file-copying process.

Slow performance occurs when you copy a single file, a folder, or multiple files

To resolve this issue, follow these steps on the client computer that has the problem:

1. Delete the third-part network provider from client computer. The default options are as follows. (Any other provider can be considered as a third party.)

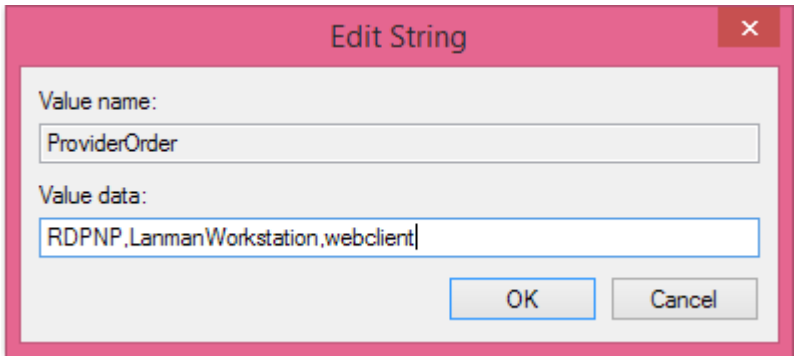


2. Remove additional values from the following registry keys. To do this, open Registry Editor. Located the following keys. Each key contains a Provider Order value.

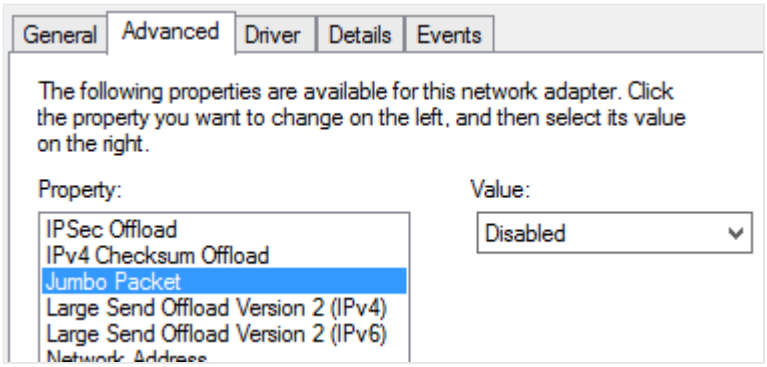
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\HwOrder`

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order`

   Check to make sure that each Provider Order value has only three values: "`RDPNP`," "`LanmanWorkstation`," and "`webclient`."

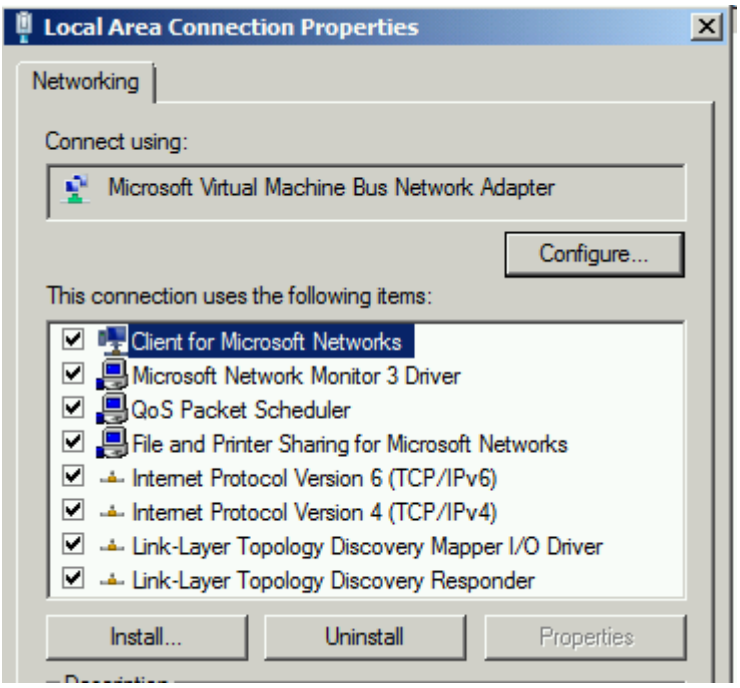


3. Compare the settings of **Jumbo Frames** and **Large send offload** with the settings on working computers. and adjust the settings of **Jumbo Frames** and **Large send offload** accordingly. (If it is disabled, enable it, and then check whether that helps)



4. Make sure that the workstation service is running.

5. Make sure that **client for Microsoft networking** is selected in the network connection properties.



Server-side troubleshooting

Install the hotfixes for the file server that hosts the shared folder.

For Windows Server 2008 or Windows 7, install all the hotfixes that are described in KB 2473205.
For Windows Server 2012 or Windows 8, install all the hotfixes that are described in KB 2899011.

If the issue isn't resolved, follow these steps to troubleshoot the issue:

1. Check whether the client is connected to a remote/WAN DFS server. (Ideally, it should be connected to the local site DFS server). If it is connected, double-check the **site and subnet** mapping in Active Directory Sites and Services. If subnets

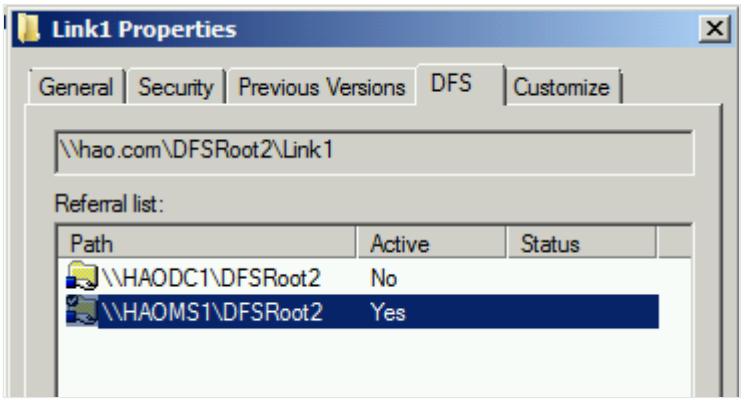
aren't mapped correctly, DFS will give an incorrect priority to remote DFS servers while it presents referrals.

2. Make sure that the local DFS server is working.
3. Set the Ordering Method for Targets in Referrals.
4. If IPv6 is enabled in the environment, configure IPv6 subnets in Active Directory Sites and Services. Or, as a workaround, disable IPv6 in the environment.

How to determine the referral DFS server to which the clients are connecting:

1. On a client computer, right-click the shared folder, and then select **Properties**.

2. On the **DFS** tab, check the referral list. The current DFS server is marked as active. In the following example, the client is connecting to the server HAOMS1.



Printing troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Printing -related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Printing sub categories

- Errors and troubleshooting: General issues
- Errors and troubleshooting: Print output or print failures
- Errors and troubleshooting: Print spooler
- Issues with Scanning
- Management and Configuration: General issues

Unable to install Secure Web Services on Devices (WSD) Printer using Print Management console

Article • 09/23/2021 • 2 minutes to read

This article helps fix an issue where you can't install a Secure Web Services on Devices (WSD) printer from Print Management Console (PrintManagement.msc) by using "Search the network for printers".

Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
Original KB number: 2701603

Symptoms

Consider the following scenario:

- You have a Secure Web Services on Devices (WSD) printer that always connects with SSL connection.
- You're unable to install the printer from Print Management Console (PrintManagement.msc) by using "Search the network for printers".

In this scenario, you try to install the printer using from following steps:

1. Open Print Management Console (`PrintManagement.msc`)
2. Expand **print servers** server name **printer** on the left pane
3. Right-click **Printer**
4. Select **Add Printer...**
5. Select **Search the network for printers**
6. Select **Secure WSD printer** on the **Network Printer Search Result**.
7. Click **Next**
8. Click **Next** to start installation.

Cause

"Search the network for printers" in Print Management Console doesn't properly use SSL to communicate with the printer.

Resolution

You can install Secure Web Services on Devices (WSD) printer from the following methods:

Method 1: From Devices and Printers using "Add a printer using a TCP/IP address or hostname"

1. Click on Start and then click Devices and Printers
2. Run Add printer Wizard
3. Click "Add a network, wireless or Bluetooth printer"
4. Click "The printer that I want isn't listed"
5. Select Add a printer using a TCP/IP address or hostname and Click "Next" button
6. Enter the printer's host name or IP address

Method 2: From Print Management console using "Add a TCP/IP or Web Services Printer by IP address or hostname"

1. Open Print Management Console (PrintManagement.msc)
2. In the Print Management console, right-click Printers and then click Add Printer
3. The Network Printer Installation Wizard starts
4. Click Add a TCP/IP or Web Services printer by IP address or hostname and then click Next
5. Enter the printer's host name or IP address (the port name will be the same by default), and then click Next
6. Make any necessary changes to the printer name, contact information, or sharing status, and then click Next

More information

Web Services on Devices (WSD) Roadmap

When attempting to add an IPP printer over HTTPS, you receive an error

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an error that occurs when you try to add an IPP printer over HTTPS.

Applies to: Windows 7 Service Pack 1
Original KB number: 2021626

Symptoms

When attempting to add an IPP printer to a Windows Vista or Windows 7 workstation over HTTPS, the queue may fail to install with the following error:

> Add Printer
> Connect to Printer
> Windows couldn't connect to the printer. Check the printer name and try again. If this is a network printer, make sure that the printer is turned on, and that the printer address is correct.

Cause

This issue occurs because Windows does not trust or cannot validate the SSL certificate being used by the print server, or the print server is using a self-signed certificate.

Resolution

This can be resolved by either:

- Configuring the print server to use a valid SSL certificate from an external certificate authority trusted by the workstation.
- If both the print server and the workstation are in the same domain, configuring the print server to use a valid SSL certificate from an enterprise certificate authority.
- If the print server is using a self-signed certificate, installing the self-signed certificate on the workstation.

How to Install an IPP Print Server's Self-Signed Certificate on a Windows Client

If your print server is using self-signed certificates, the following steps can be used to install the self-signed certificate on the client(s) so they are able to use the printer.

> ⓘ **Note**
>
> This should only be performed for SSL certificates from servers you trust.

1. Log on to the client as an administrator
2. Find Internet Explorer in the start menu, right-click on it, and click **Run as administrator**.
3. In Internet Explorer, browse to the Print Server using HTTPS (for example, `https://PrintServerName/`)
4. In the address bar, the words "Certificate Error" should appear on the right side next to a Red shield icon - click on the error.
5. Click **View Certificates**.
6. On the certificate window, click **Install Certificate...**.
7. Select **Place all certificates in the following store**.
8. Click **Browse...**.
9. Select **Trusted Root Certification Authorities** and click **OK**.
10. Click **Next**, then click **Finish**.
11. A security warning will appear that you are adding a certificate from a source that cannot be validated. Click **Yes** to trust this SSL certificate.
12. Close Internet Explorer.
13. The printer can now be installed.

Two-sided (duplex) printing options cannot be set for applications in Windows 8.1 and Windows 8

Article • 09/23/2021 • 2 minutes to read

This article provides workarounds for an issue where two-sided (duplex) printing options can't be set for applications.

Applies to: Windows 10 - all editions
Original KB number: 3022505

Symptoms

When this issue occurs, the printed documents do not respect the settings that you deployed in the duplex printing options.

Cause

This issue occurs because the duplex printing options currently use the Device charm setting.

Workaround

To work around this issue, follow these steps to change the duplex printing options.

Windows 8

1. Open the item that you want to print.
2. Swipe in from the right edge of the screen, tap Devices, and then tap Print. If you are using a mouse, point to the lower-right corner of the screen, move up the mouse pointer, click Devices, and then click Print.
3. Select a printer from the list. You can now see a preview of the item.
4. When **Duplex printing** is displayed in this pane, you can change the settings. Otherwise, tap or click **More settings**. When **Duplex printing** is displayed, you can change the settings.
5. Tap or click Print to print the item.

> **Note**
>
> If the Duplex printing option is never displayed in step 4, the printer device may be unable to use duplex printing options. You can retry, by using another printer and starting from step 3.

Windows 8.1

1. Open the item that you want to print.
2. Swipe in from the right edge of the screen, tap **Devices**, and then tap **Print**. If you are using a mouse, point to the lower-right corner of the screen, move up the mouse pointer, click **Devices**, and then click **Print**.
3. Select a printer from the list. You can now see a preview of the item.
4. When **Duplex printing** is displayed in this pane, you can change the settings. Otherwise, tap or click **More settings**. When **Duplex printing** is displayed, you can change the settings.
5. To set duplex printing as the default setting for the selected printer, select the **Use these settings in all applications** option.
6. Tap or click **Print** to print the item.

> **Note**
>
> If the Duplex printing option is never displayed in step 4, the printer device may be unable to use duplex printing options. You can retry by using another printer and starting from step 3.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the "Applies to" section.

More information

To learn more about how to print more detail, see How to print in Windows 8.1.

PNG images don't print correctly in Word 2010 after the system display scaling setting is changed in Windows 7

Article • 09/23/2021 • 2 minutes to read

This article discusses an issue in which PNG images don't print correctly in Word 2010 after the scaling setting for the system display is changed in Windows 7.

Applies to: Windows 7 Service Pack 1
Original KB number: 3101023

Symptoms

Consider the following scenario:

- You have a Windows 7-based computer that has Microsoft Word 2010 installed.
- You have a Word document that contains a PNG image.
- In Control Panel, you change the Windows display scaling from the default setting of **Smaller - 100% (default)** to **Medium - 125%**.
- In Word, you print the document to an XPS-based printer driver.

After you print the Word document, you notice that the edges of PNG image are cut off on the printout.

Cause

This issue may occur because the PNG image doesn't contain the pHYs (physical pixel dimensions) chunk to specify the size of each pixel in the image.

Workaround

To work around this issue, follow these steps:

1. Start Word 2010.
2. Right-click the PNG image, and then click **Format picture**.
3. Change any of the **Sharpen and Soften** or **Brightness and Contrast** slider settings.
4. Click **Close** to save the changes.
5. Right-click the PNG image again, and then revert the slider settings to their original positions.

6. Click **Close** to save the changes.

This change in the image settings adds the pHYs chunk to the PNG image and enables it to print correctly.

Print directly to the printer setting doesn't work with XPS-based print drivers

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where the **Print directly to the printer** option doesn't work with XPS-based print drivers.

Applies to: Windows 7 Service Pack 1
Original KB number: 3017432

Symptoms

Consider the following scenario:

- On a Windows 7 Service Pack 1-based system, you have a printer installed that uses an XPS-based print driver.
- On the **Advanced** tab of the printer properties, the **Print directly to the printer** option is selected.

In this scenario, print jobs do not print.

Cause

When the **Print directly to the printer** option is selected, the print job must be rendered under the application process. However, with XPS-based print drivers, the print job is rendered under the PrintFilterPipelineSvc.exe process. Therefore, the print job must be sent to the spooler, where it is then sent to the PrintFilterPipelineSvc.exe process to be rendered.

Workaround

To work around this issue, use one of the following methods:

- Configure the printer to use spooling.
- Use a GDI-based print driver.

More information

Windows 8 and Windows 8.1 use the new v4 XPS-based printer model. Therefore, the **Print directly to the printer** option is unavailable (appears dimmed).

"Server Busy" error message when you try to scan a document

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution for fixing "Server Busy" error when you try to scan a document.

Applies to: Windows 10 - all editions
Original KB number: 2971655

Symptoms

Consider the following scenario:

- You are running a 64-bit (x64) version of Windows 8.1, Windows 8, or Windows 7.
- You are running a 32-bit scanning application.
- You are using a scanner that uses the TWAIN 1.0 default interface.
- You try to scan a document.

In this scenario, you are prompted by a "What do you want to scan?" message. The message window also displays options to configure the scanner. After several seconds, you receive the following error message:

> Server Busy

Cause

This problem occurs because a 32-bit scanning application is running in a 64-bit version of Windows. In this situation, the drivers for the scanner are loaded during a separate Wiawow64.exe process. The "What do you want to scan?" message is part of the Wiawow64 process. The error message is caused by an OLE call from the 32-bit scanning application. This problem occurs because the OLE call has a time-out value that expires while the scanning application is waiting for user input in the "What do you want to scan?" window.

Resolution

To resolve this problem, we recommend that you contact the scanning application vendor to have them update the application.

More information

If you are a developer, see the following information:

When you call the AfxOleInit(); function, the *m_nTimeout* parameter is set to a default value of 8 seconds. To disable the time-out of the OLE call, you must add the following line after you call the AfxOleInit(); function:

```
AfxOleGetMessageFilter()->EnableNotRespondingDialog(FALSE);
```

Scanning using a scanner may cause a TWAIN aware application to hang

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution for the issue that scanning using a scanner may cause a TWAIN aware application to hang.

Applies to: Windows 7 Service Pack 1
Original KB number: 982436

Source: Microsoft Support

Rapid publishing

Rapid publishing articles provide information directly from within the microsoft support organization. The information contained herein is created in response to emerging or unique topics, or is intended supplement other knowledge base information.

Symptoms

When a 32-bit TWAIN aware application scans using a WIA driver on a 64-bit Windows Vista or Windows 7 system, the TWAIN application may stop responding.

Cause

If you leave the scan dialog open for about 10 minutes before you push the [Scan] button, the message used to transfer the scanned image from the WIA driver to the TWAIN application is not sent to the TWAIN application.

Resolution

This problem can be avoided by doing either of the followings:

- Scan image soon after you open the scan dialog.
- Use a WIA aware application, not a TWAIN aware application.

More information

This behavior is by design.

Disclaimer

Microsoft and/or its suppliers make no representations or warranties about the suitability, reliability, or accuracy of the information contained in the documents and related graphics published on this website (the "materials") for any purpose. The materials may include technical inaccuracies or typographical errors and may be revised at any time without notice.

To the maximum extent permitted by applicable law, Microsoft and/or its suppliers disclaim and exclude all representations, warranties, and conditions whether express, implied, or statutory, including but not limited to representations, warranties, or conditions of title, non infringement, satisfactory condition or quality, merchantability and fitness for a particular purpose, with respect to the materials.

How to add the print directory feature to Windows Explorer

Article • 09/23/2021 • 2 minutes to read

This article describes how to add the print directory feature, and how to enable printing of the directory listing from within Windows Explorer.

Applies to: Windows 10 - all editions, Windows Vista
Original KB number: 272623

Summary

For more information about How to add the Print Directory feature for folders in Windows XP, in Windows Vista, or in Windows 7, click the following article number to view the article in the Microsoft Knowledge Base: 321379 How to add the Print Directory feature for folders in Windows XP, in Windows Vista, or in Windows 7

More information

To add the print directory feature to Windows Explorer, follow these steps:

Step 1: Create the Printdir.bat file

To do this, follow these steps:

1. Click **Start**, click **Run**, type *notepad*, and then click **OK**.
2. Paste the following text into Notepad:

```
Console

@echo off
dir %1 /-p /o:gn > "%temp%\Listing"
start /w notepad /p "%temp%\Listing"
del "%temp%\Listing"
exit
```

3. On the **File** menu, click **Exit**, and then click **Yes** to save the changes.
4. In the **Save As** dialog box, type the following text in the **File name** box, and then click **Save**: %windir%\Printdir.bat

> **Note**
>
> If you receive a dialog box that states that you do not have permission to save in this location, you can save the file to the desktop. Next, you click **Start**, click **Run**, type *%windir%*, and then click **OK**. Then, you can copy the file from the desktop to the location.

Step 2: Edit the registry

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base: 322756 How to back up and restore the registry in Windows

1. Click **Start**, click **Run**, type *Notepad*, and then click **OK**.
2. Type the following commands in Notepad.

```registry
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\Directory\Shell]
@="none"

[HKEY_CLASSES_ROOT\Directory\Shell\Print_Directory_Listing]
@="Print Directory Listing"

[HKEY_CLASSES_ROOT\Directory\shell\Print_Directory_Listing\command]
@="Printdir.bat \"%1\""

[HKEY_CLASSES_ROOT\SOFTWARE\Classes\Directory]
"BrowserFlags"=dword:00000008

[HKEY_CLASSES_ROOT\SOFTWARE\Classes\Directory\shell\Print_Directory_Lis
ting]
@="Print Directory Listing"

[HKEY_CLASSES_ROOT\SOFTWARE\Classes\Directory\shell\Print_Directory_Lis
ting\command]
```

```
@="Printdir.bat \"%1\""

[HKEY_CURRENT_USER\Software\Microsoft\Windows\Shell\AttachmentExecute\
{0002DF01-0000-0000-C000-000000000046}]
@=""

[HKEY_CLASSES_ROOT\SOFTWARE\Classes\Directory]
"EditFlags"="000001d2"
```

On the **File** menu, click **Save As**.

3. In the **Save in** list, click **Desktop**.
4. In the **File name** box, type *PrintDirectoryListing.reg*, click **All Files** in the **Save as type** list, and then click **Save**.
5. On the desktop, double-click the LoggingOn.reg file to add the registry keys to the Windows registry.
6. Click **OK** in the message box.

How to Alter Behavior of Printers That Roam with Roaming Profiles

Article • 09/23/2021 • 3 minutes to read

This article describes how to alter a behavior of printers that roams with roaming profiles.

Applies to: Windows 10 - all editions
Original KB number: 304767

Important

This article contains information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. For information about how to back up, restore, and edit the registry, click the following article number to view the article in the Microsoft Knowledge Base:

256986 Description of the Microsoft Windows Registry

Summary

By design, when a user is using a roaming profile, that user's default printer roams with the user profile. However, in some environments this may not be the desired behavior. This article provides methods you can use to alter this behavior.

More information

Warning

If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

Important

The information in this article is designed for use by corporate administrators. Before you use any of the methods that are described in this article in your environment, you should thoroughly test the method in a test environment.

Printers are designed to roam with a user's roaming profile, and this is why the default printer is stored under the HKEY_CURRENT_USER branch of the registry. To alter this behavior, use either of the following methods.

Method 1

Export the default printer setting for an already-installed printer, and then merge the setting into the user's profile when the user logs on to the computer:

1. Use Registry Editor (Regedit.exe) to export the following registry key:

   `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows`

2. Modify the registry (.reg) file you made in step 1 with a text editor so that the only registry value name below the key is:

   "Device"=...

   > **Note**
   >
   > The registry file should contain a blank line at the bottom of the file.

3. Use Registry Editor (Regedit.exe) to add a new ResetPrinter string value under the following registry key:

   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

4. The value of the ResetPrinter value should be something similar to the following value:

   REGEDIT.EXE -S *path**File.reg*
   where *File.reg* is the name you used to store the default printer.

Method 2

If computers in a specific area contain similar computer names, you can use a .vbs script file that matches a specific set of characters in the computer name, and installs a corresponding printer. The sample code that is included in this method only requires

that you modify the IF lines. For example, the first IF statement in the code translates to "if the computer name contains the text "LAB1-", then set the default printer to "\\LAB1\LaserJet". To complete this method:

1. Copy the following sample VBS code into a. vbs file, for example, Defaultprinter.vbs:

```
Visual Basic Script

Option Explicit
DIM RegEntry, ComputerName

RegEntry="HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerNa
me\ComputerName" ComputerName = ReadRegValue(RegEntry)

if InStr(1,ucase(ComputerName),"LAB1-",vbTextCompare) > 0 then call
SetPrinter("\\LAB1\LaserJet")
if InStr(1,ucase(ComputerName),"LAB2-",vbTextCompare) > 0 then call
SetPrinter("\\LAB2\LaserJet")
if InStr(1,ucase(ComputerName),"OFFICE-",vbTextCompare) > 0 then call
SetPrinter("\\OFFICE\LaserJet")
'so on and so forth.
wscript.quit

'*** This subroutine installs and sets the default printer
Sub SetPrinter(ByVal PrinterPath)
    DIM WshNetwork
    Set WshNetwork = CreateObject("WScript.Network")
    WshNetwork.AddWindowsPrinterConnection(PrinterPath)
    WshNetwork.SetDefaultPrinter Printerpath
end sub

'**** This function returns the data in the registry value
Function ReadRegValue(ByVal RegValue)
    DIM WSHShell
    Set WSHShell = WScript.CreateObject("WScript.Shell")
    ReadRegValue=""
    On Error Resume Next
    ReadRegValue= WSHShell.RegRead(RegValue)
End Function
```

2. Modify the IF lines as needed. The only portion of the IF lines that need to be modified is between double quotes. You may need to add additional IF lines.

3. Use Registry Editor to create a ResetPrinter string value under the following registry key:

   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

4. The value of ResetPrinter should be something similar to the following value:

WSCRIPT.EXE *path*\DefaultPrinter.vbs
where *path* is the location where the Defaultprinter.vbs file is stored.

> **Note**
>
> It is also possible to run the Defaultprinter.vbs file from a login script instead of the run key. Both of the methods that are described in this article reset the default printer that a user's profile is set to print to. Also, if the sample script that is included in this article does not run properly, you may need to upgrade or install the Windows Scripting Host.
>
> Microsoft provides programming examples for illustration only, without warranty either expressed or implied. This includes, but is not limited to, the implied warranties of merchantability or fitness for a particular purpose. This article assumes that you are familiar with the programming language that is being demonstrated and with the tools that are used to create and to debug procedures. Microsoft support engineers can help explain the functionality of a particular procedure, but they will not modify these examples to provide added functionality or construct procedures to meet your specific requirements.

Error 0x00000709 when you use a CNAME record for a print server in Windows Server 2008 R2: Operation could not be completed

Article • 09/23/2021 • 2 minutes to read

This article helps fix the error 0x00000709 (Operation could not be completed). The error occurs when you use a CNAME record for a print server.

Applies to: Windows Server 2012 R2
Original KB number: 2546625

Symptoms

Consider the following scenario:

- You have printers that are hosted on a system that is running Windows Server 2008 R2.
- You provide an alternative UNC path for the print server. And you decide to do so by using a CNAME (alias) resource record in DNS.
- Clients try to connect to the printers by using the CNAME record in the UNC path.

In this scenario, clients can't connect to the printers if they use the CNAME record in the UNC path. Besides, attempts to connect to the shared printers fail with the following error:

> Operation could not be completed (error 0x00000709). Double check the printer name and make sure that the printer is connected to the network.

Note

- Attempts to connect to the printers succeed as long as you use the actual host name instead of the CNAME record.
- After you implement the DnsOnWire registry value that is described in the following article in the Microsoft Knowledge Base, the problem persists: **Error message when you try to connect to a printer by using an alias (CNAME) resource record: "Windows couldn't connect to the printer"**

Cause

This issue may occur if certain non-Microsoft DNS solutions are providing name resolution for the network.

Resolution

To work around this issue, follow these steps on the print server, and then restart the Print Spooler service:

1. Implement the `DnsOnWire` registry value that's described in the following article:

   Error message when you try to connect to a printer by using an alias (CNAME) resource record: "Windows couldn't connect to the printer"

2. Edit the local Hosts file to include the CNAME record for the server.

   > **Note**
   >
   > The Hosts file entry must be entered as a NetBIOS name instead of as an FQDN.

The following example is for illustration only. Use names and IP addresses that are valid for your network.

Use NetBIOS name: 192.168.0.10 CNAME

Don't use FQDN: 192.168.0.10 `CNAME.CONTOSO.COM`

More information

The issue that is described in the Symptoms section may occur if the non-Microsoft DNS solution provides `QRecord` responses of type ALL.

Errors when you connect to a shared printer by using a CNAME record

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution for fixing the errors when you connect to a shared printer by using a CNAME record.

Applies to: Windows Server 2012 R2, Windows 7 Service Pack 1
Original KB number: 2965564

Summary

This article describes two error messages that occur when you connect to a shared printer by using a CNAME record.

Symptoms

Error 1

You provide an alternative Universal Naming Convention UNC (UNC) path for a Windows Server 2008 R2-based printer server. The UNC path uses a CNAME DNS record. The following error message is received when clients try to connect to the printer:

> Operation could not be completed (error 0x00000709). Double-check the printer name and make sure that the printer is connected to the network.

For more information about this issue, click the following article number to view the article in the Microsoft Knowledge Base:

> 2546625 "Operation could not be completed (error 0x00000709)" error when you use a CNAME record for a print server in Windows Server 2008 R2

Error 2

Clients receive the following error message when you use a CNAME DNS record to connect to a printer server that is running Windows Server 2008 R2 or Windows 7:

> Windows couldn't connect to the printer. Check the printer name and try again. If this is a network printer, make sure that the printer is turned on, and that the printer address is correct.

For more information about this issue, click the following article number to view the article in the Microsoft Knowledge Base:

> 979602 Error message when you try to connect to a printer by using an alias (CNAME) resource record: "Windows couldn't connect to the printer"

Resolution

To resolve these issues, use the following commands:

```
reg add hklm\system\currentcontrolset\control\print /v DnsOnWire /t
REG_DWORD /d 1
reg add hklm\system\currentcontrolset\services\lanmanserver\parameters /v
DisableStrictNameChecking /t REG_DWORD /d 1
reg add hklm\system\currentcontrolset\services\lanmanserver\parameters /v
OptionalNames /t REG_SZ /d " aliasname "
```

Note

For third-party DNS providers, you may have to use QWord instead of DWord . Therefore, you should use QWord instead of DWord for these commands.

Printing from Modern App creates large spool file when you select Advanced Printing features

Article • 09/23/2021 • 2 minutes to read

This article describes an issue that occurs when you print from Modern App as this creates a large spool file when you select Advanced Printing features such as number of pages per sheet.

Applies to: Windows 10 - all editions
Original KB number: 2989058

Symptoms

Consider the following scenario:

- You have a system that is running Windows 10.
- You have a document open in a Modern App that contains images and text on multiple pages, for example a PDF file.
- You try to print the file by using a PostScript or PCL6-based printer driver.
- Within the printer properties, you select the print feature to include more than one page per sheet.

In this scenario when the print job is sent to the print queue, you may notice that the size of the print job is larger than the file size.

Cause

This issue is expected behavior as the spooled data has to be converted from XPS data to an Enhanced MetaFile (EMF). This is so that data can be converted by the GDI engine into the Printer Definition Language (PDL) data that the print device can then receive.

In some cases, the JPEG pass-through won't be used, as rotation of JPEG images is unsupported in this scenario.

Resolution

To work around this issue, you have to limit the size of the spooled data. Print the documents from a desktop application as there will be no data conversion required for

the print device.

RPC connection updates for print in Windows 11

Article • 10/24/2022 • 5 minutes to read

Applies to: Windows 11, version 22H2 and later versions of Windows

Windows 11, version 22H2 introduces changes to print components that modify how Windows machines communicate with each other during printing or print related operations. For example, the changes come into effect when you print to a printer shared out by a print server or another computer on the network. These changes were made to further improve the overall security of printing in Windows. The default configuration of the RPC connection settings enforces newer and more secure communication methods. Home users and enterprise administrators can also customize the settings for their environment.

Update details

- For print related communications, by default, RPC over TCP is used for client – server communications.
  - Using RPC over Named Pipes for print related communication between computers is still available but is disabled by default.
  - Using RPC over TCP or RPC over Named Pipes for print related communication can be controlled by Group Policy or through the registry.
- By default, the client or server only listens for incoming connections via RPC over TCP.
  - The Spooler service can be configured to also listen for incoming connections via RPC over Named Pipes. This isn't the default configuration.
  - This behavior can be controlled by Group Policy or through the registry.
- When RPC over TCP is used, a specific port can be configured to use for communication instead of dynamic ports.
- Environments in which all computers are domain joined and support Kerberos can now enforce Kerberos authentication.

Recommendations on configuring an environment

The following contains recommendations on how to properly configure the environment to avoid or resolve issues with communication between computers.

Allow RPC over TCP communication

The most common issue is that firewall rules are preventing communication between the computers. To resolve issues with the firewall, follow these steps:

1. Ensure that the RPC Endpoint Mapper port (135) isn't blocked.
2. Open up the high range ephemeral ports (49152 – 65535) on the server or follow the guidance in the Configuring RPC to use certain ports section below to specify a range of ports for RPC.

For more information on the different ports, and their usage by system services, see Service overview and network port requirements for Windows.

Using RPC over Named Pipes

This configuration isn't recommended. However, it can be used if RPC over TCP isn't an option in the current environment.

- To enable a Windows 11, version 22H2 computer to use RPC over Named Pipes instead of RPC over TCP for communication, see the Use RPC over Named Pipes for client - server communication section.
- To enable a Windows 11, version 22H2 computer to listen for incoming connections via RPC over Named Pipes and RPC over TCP, see the Enable listening for incoming connections on RPC over Named Pipes section

The following additional configurations might also be needed to properly support RPC over Named Pipes in the environment.

- Set the **RpcAuthnLevelPrivacyEnabled** registry value to **0** on the server/host machine. See Managing deployment of Printer RPC binding changes for CVE-2021-1678 (KB4599464) (microsoft.com)
- Some scenarios also require guest access in SMB2/SMB3, which is disabled by default. To enable it, see Guest access in SMB2 and SMB3 disabled by default in Windows

Configuring RPC to use certain ports

See How to configure RPC to use certain ports and how to help secure those ports by using IPsec.

- To set a dynamic/excluded port range, run the `netsh int` commands.
- To use IPSec with netsh, run the `netsh ipsec` commands.
- To use Windows Firewall to block a range of ports, run the `netsh advfirewall` commands.

All of the above are viable solutions. However, some solutions may be easier than the ones that require you to set the rule for each port (IPSec and AdvFirewall). For testing purpose, you may use the dynamic/excluded port range method since you can specify the range. For example:

To restrict dynamic port range, run these commands:

Console

```
netsh int ipv4 show dynamicport tcp
netsh int ipv4 show dynamicport udp
netsh int ipv4 set dynamicportrange tcp startport=50000 numberofports=255
netsh int ipv4 set dynamicportrange udp startport=50000 numberofports=255
netsh int ipv6 set dynamicportrange tcp startport=50000 numberofports=255
netsh int ipv6 set dynamicportrange udp startport=50000 numberofports=255
```

Then, restart the computer.

> ⓘ **Note**
>
> 255 is the minimum number of ports can set.

To further restrict port range, run these commands:

Console

```
netsh int ip show excludedportrange tcp
netsh int ip show excludedportrange udp
netsh int ipv4 add excludedportrange tcp startport=50000 numberofports=225
netsh int ipv4 add excludedportrange udp startport=50000 numberofports=225
netsh int ipv6 add excludedportrange tcp startport=50000 numberofports=225
netsh int ipv6 add excludedportrange udp startport=50000 numberofports=225
```

Then, restart the computer.

> ⓘ **Note**
>
> If you restrict the number of ports too much then services on the system will not be able to communicate effectively and can cause an issue with functionality.

Configuring RPC communication for Windows Print components

The following settings can be configured through either Group Policy or directly through the registry to achieve the desired effect. Refer to the documentation in the Group Policy editor for specific details on each setting.

Use RPC over Named Pipes for client – server communication

- Enable by using Group Policy:
  Path: **Computer Configuration** > **Administrative Templates** > **Printers** > **Configure RPC connection Settings**
  Enable and set to **RpcOverNamedPipes**.
- Enable the setting by using the registry:
  Run `reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RPC" /v RpcUseNamedPipeProtocol /t REG_DWORD /d 1 /f`

Enable listening for incoming connections on RPC over Named Pipes

- Enable via Group Policy:
  Path: Computer Configuration > Administrative Templates > Printers > Configure RPC listener settings
  Enable and set protocols allowed to be used to **RpcOverNamedPipesAndTcp**.
- Enable the setting via the registry:
  Run `reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RPC" /v RpcProtocols /t REG_DWORD /d 0x7 /f`

Use a specific port for RPC over TCP communication

- Enable via Group Policy:
  Path: **Computer Configuration** > **Administrative Templates** > **Printers** > **Configure RPC over TCP port** Enable and set the port number
- Enable the setting via the registry
  Run `reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RPC" /v RpcTcpPort /t REG_DWORD /d <port number> /f`

Max port: 65535

Enforce Kerberos authentication

- Enable via Group Policy:
  Path: **Computer Configuration** > **Administrative Templates** > **Printers** > **Configure RPC listener settings**
  Enable and set the authentication protocol allowed to be used to Kerberos.
- Enable the setting via the registry
  Run `reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\RPC" /v ForceKerberosForRpc /t REG_DWORD /d 1 /f`

Error message when you try to install a network printer in Windows 7: "0x0000052e"

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround to an error "0x0000052e" that occurs when you try to install a network printer in Windows 7.

Applies to: Windows 7 Service Pack 1
Original KB number: 2269296

Symptoms

When you try to install a network printer on a computer that is running Windows 7, you receive the following error message:

> Windows cannot connect to the printer (details: Operation failed with error 0x0000052e)

Cause

This problem can occur if the credentials on the Windows 7 client do not match the credentials that are stored on the print server. Error message "0x0000052e" indicates the following error:

> "Logon failure: unknown user name or bad password."

Workaround

To work around this problem, use either of the following methods.

Workaround 1

Before you add the network printer, open a **Command Prompt** window, and type the following at the **Command Prompt**:

```
Console

start \\<servername>\<printername>
```

> **Note**
>
> In this command, <servername> represents the name of the print server and <printername> represents the share name of the printer.

In the authentication window, enter the appropriate credentials.

Workaround 2

Store a trusted credential in **Credential Manager**. To do this, follow these steps:

1. In **Control Panel**, open **Credential Manager**.
2. Click **Add a Windows credential**.
3. In the dialog box, enter an appropriate print server name. Then, enter a user name and password that are trusted on the print server.
4. Click **OK**.

More Information

This behavior is different in earlier Windows versions. In those versions, you are prompted for credentials if the connection fails because of an unknown user name or a bad password.

Not all printer drivers downloaded from Windows Update are listed in Add Printer wizard

Article • 12/06/2021 • 2 minutes to read

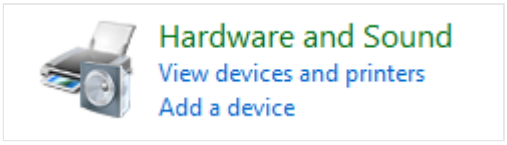
This article provides a workaround for an issue in which not all printer drivers that are downloaded from Windows Update are listed in the Add Printer wizard.

Applies to: Windows 10 - all editions, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2
Original KB number: 4508350

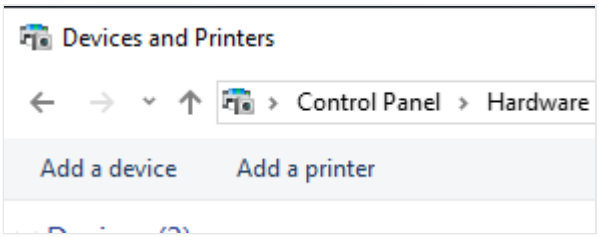
Symptoms

On a computer that is running Windows 10, version 1803, Windows Server, version 1803 or a later version of Windows, you do the following operations:

1. Select **Start**, type *Control Panel*, and then press Enter.
2. In Control Panel, select the **View Devices and Printers** item.

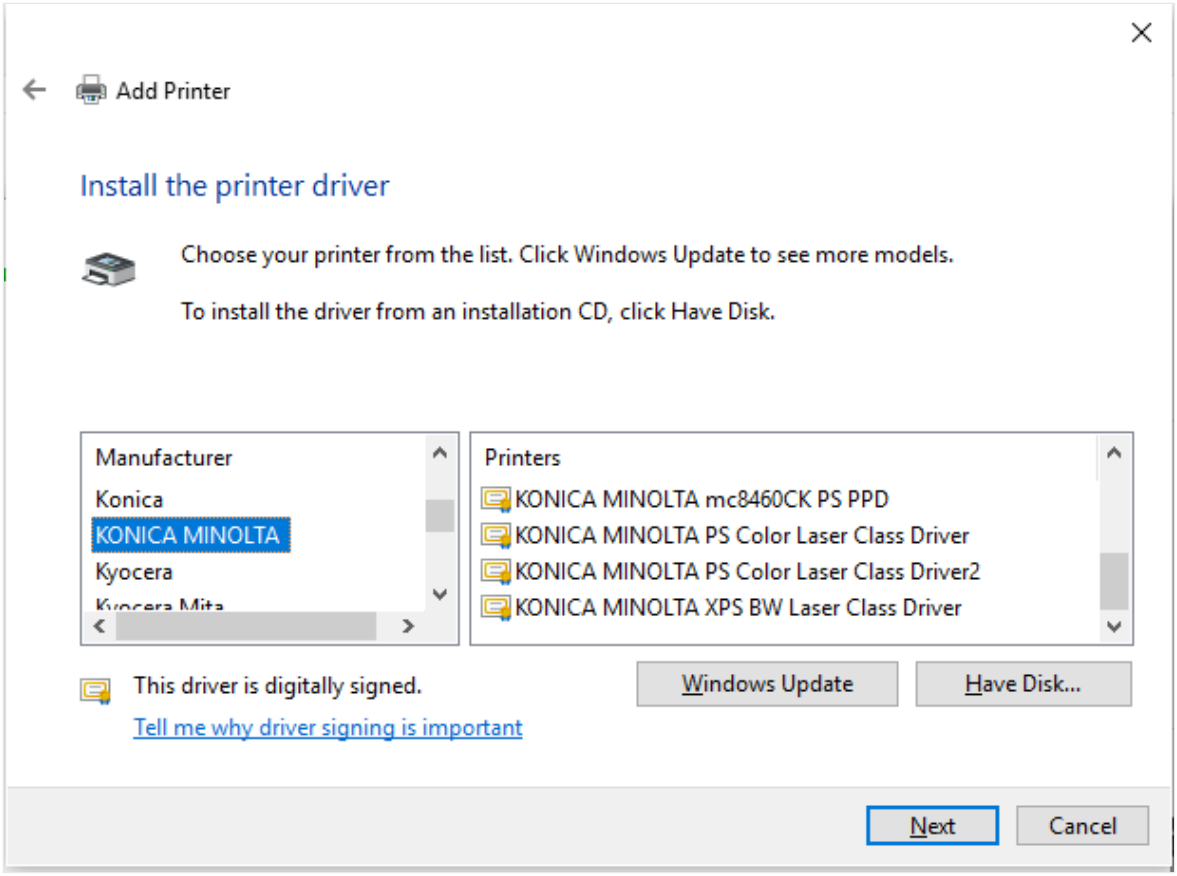


3. Select **Add Printer** at the top of the window.



4. After the wizard started, select **The printer that I want isn't listed**.
5. Select **Add a local printer or network printer with manual settings**, and then select **Next**.
6. On the **Choose a Printer Port** page, select the desired port, and then select **Next**.
7. On the **Install the printer driver** page, select **Windows Update**.

8. The updated **Printers** list is displayed from Windows Update. For example, if you select **KONICA MINOLTA** under **Manufacturer**, the **Printers** list is displayed as follows.



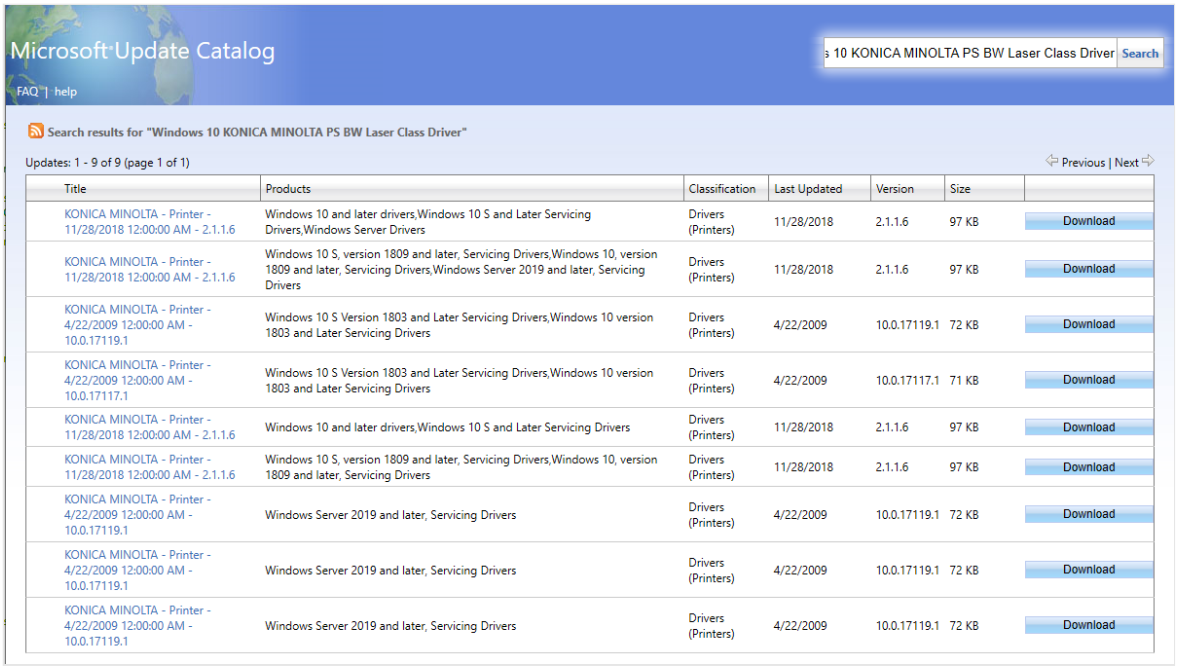
In this scenario, not all registered drivers are displayed.

For example, "KONICA MINOLTA PS BW Laser Class Driver" and "KONICA MINOLTA PS Color Laser Class Driver" are not both displayed as expected.

Workaround

To work around this issue, manually download and install the printer driver to be installed from the Windows Update Catalog. In the example of the driver mentioned in the Symptoms section, install according to the following procedure.

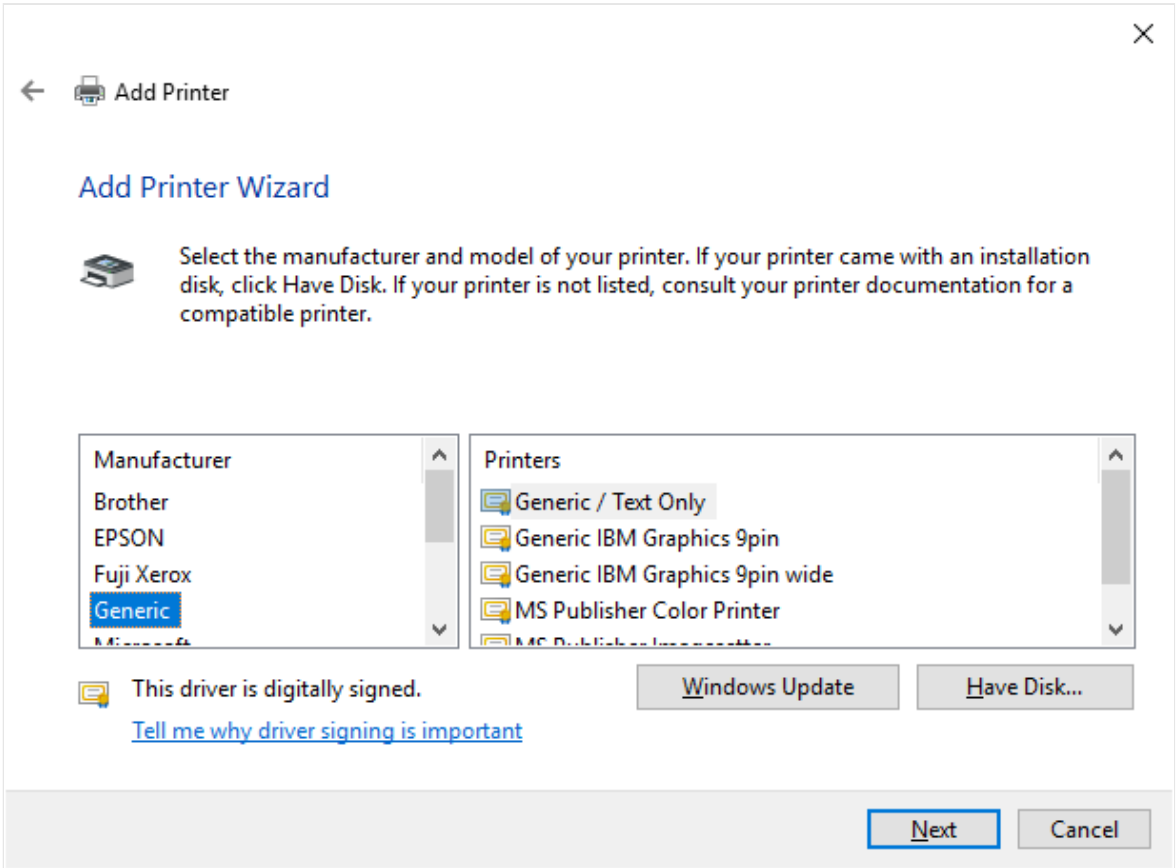
1. Go to the Windows Update Catalog.
2. In the search box, enter the keyword of the driver to be downloaded, such as "Windows 10 KONICA MINOLTA PS BW Laser Class Driver," and then select **Search**.
3. After the list is displayed, select the **Download** button for the target driver, and save it to any folder.



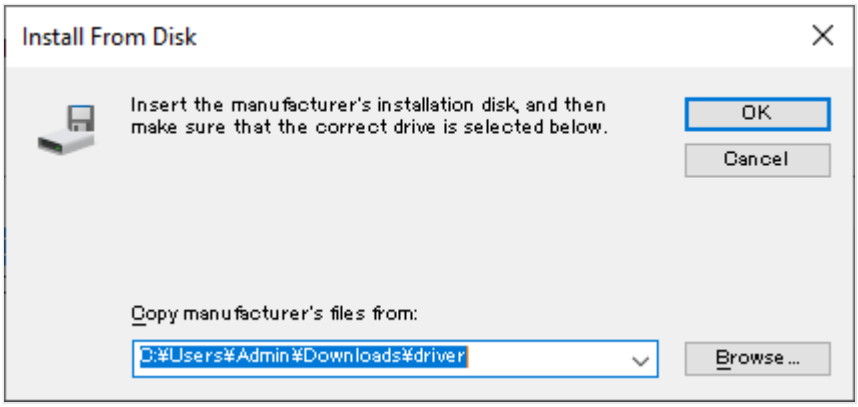
4. Extract the saved .cab file to any folder.

5. Do steps 1 through 6 in the Symptoms section.

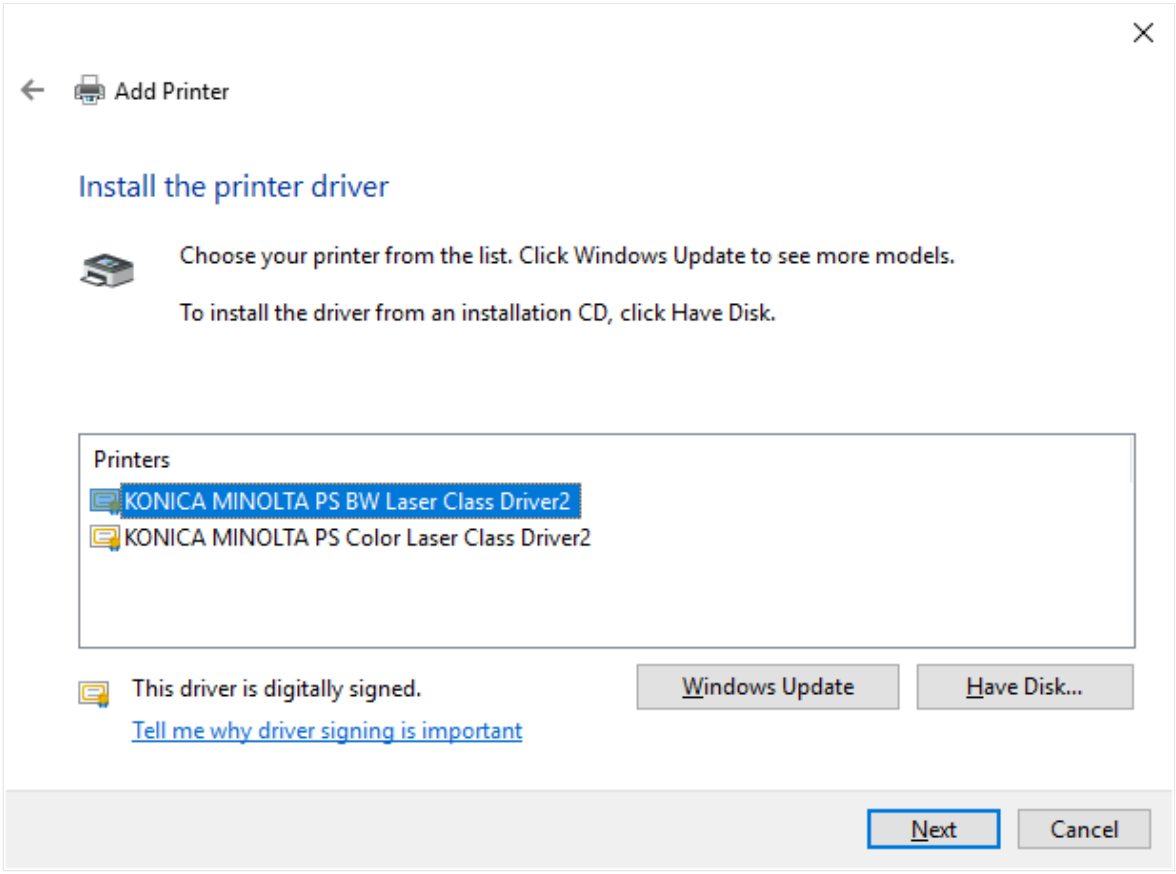
6. On the **Install the printer driver** screen, select **Have disk**.



7. Browse to the folder that was extracted in step 4, and then select the **OK**.



8. After the printer driver list appears, select the target driver, and then select **Next** to go through the remaining wizard steps and complete all installation tasks. Contact your printer vendor for more information about which printer driver must be downloaded for the printer that you are using.



Print driver default settings are not inherited through "Point and Print" in Windows 10 Version 1709

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to the issue in which print driver default settings are not inherited through "Point and Print" in Windows 10 Version 1709.

Applies to: Windows Server 2019, Windows Server 2016, Windows 10, version 1709
Original KB number: 4052855

Symptoms

Consider the following scenario:

- You have a client that is running Windows 10 Version 1709 or Windows Server Version 1709.
- You have a print server that is running Windows Server 2016, Windows Server 2012, or Windows Server 2012 R2, or Windows Server 2008 R2.
- You install printer drivers by using the "Point and Print" process.

In this scenario, the client does not inherit default settings from the print server.

Cause

This issue occurs because of a mismatch in the universal driver (or PScript5 driver) between the print server and the client.

Resolution

To fix this issue, set the printer settings manually on the client following these steps:

1. Right-click the **Start** button, and then select **Settings**.
2. Select **Devices**.
3. In the center of the **Devices** window, select **Devices and printers**.
4. In the **Devices and Printers** window, right-click the icon of a printer that you installed from the server computer. Then, select **Printing preferences**.

> ⓘ Note
>
> The **Printing Preferences** dialog box opens.

5. In the dialog box, select the **Advanced** button.

> ⓘ Note
>
> The **Advanced Options** dialog box opens. You can change the printer settings in this dialog box.

Status

Microsoft has confirmed that this is an issue in the Microsoft products that are listed in the "Applies to" section.

This issue has been fixed in Windows 10, version 1803 and Windows Server, version 1803.

Remote Desktop Services troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Remote Desktop Services-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Remote Desktop Services sub categories

- Administration
- Connecting to a session or desktop
- Redirection (not printer)
- Remote desktop sessions

Description of Remote Server Administration Tools

Article • 09/23/2021 • 3 minutes to read

This article describes the tools that are available for installation as part of Remote Server Administration Tools.

Applies to: Windows Server 2012 R2, Windows 7 Service Pack 1
Original KB number: 958830

Introduction

This article describes the tools that are available for installation as part of Remote Server Administration Tools for Windows 7. Tools in this package can be used to manage technologies that run on Windows Server 2008 R2. They can also be used to manage some technologies that run on Windows Server 2003, Windows Server 2003 R2, or Windows Server 2008.

More information

Remote Server Administration Tools technology	**Description**	**Manages technology on Windows Server 2003**	**Manages technology on Windows Server 2008**
Active Directory Certificate Services Tools	Active Directory Certificate Services Tools include: • Certification Authority • Certificate Templates • Enterprise PKI • Online Responder Management snap-ins	√, except Online Certificate Status Protocol (OCSP)	√

Remote Server Administration Tools technology	Description	Manages technology on Windows Server 2003	Manages technology on Windows Server 2008
Active Directory Domain Services (AD DS) Tools and Active Directory Lightweight Directory Services (AD LDS) Tools	AD DS Tools include: • Active Directory Users and Computers • Active Directory Domains and Trusts • Active Directory Sites and Services • Active Directory Administrative Center (ADAC) • Server for Network Information Service (NIS) tools • Windows PowerShell module for Active Directory • Other snap-ins and command-line tools for remotely managing AD DS AD LDS Tools include: • Active Directory Sites and Services • ADSI Edit • Schema Manager • Other snap-ins and command-line tools for managing AD LDS Server for NIS Tools includes: • An extension to the Active Directory Users and Computers snap-in • The Ypclear.exe command-line tool	√, Windows PowerShell and ADAC remote management require the Active Directory Web Service download package.	√, PowerShell and ADAC remote management require the Active Directory Web Service download package.
BitLocker Active Directory Recovery Password Viewer	The BitLocker Active Directory Recovery Password Viewer tool is an extension for the Active Directory Users and Computers Microsoft Management Console (MMC) snap-in. Using this tool, you can open a computer object's **Properties** dialog box to view the corresponding BitLocker recovery passwords.	Not available	Not available
DHCP Server Tools	DHCP Server Tools include the DHCP Management Console, and the Netsh command-line tool.	√	√
DNS Server Tools	DNS Server Tools include the DNS Manager snap-in, and the Ddnscmd.exe command-line tool.	√	√

Remote Server Administration Tools technology	Description	Manages technology on Windows Server 2003	Manages technology on Windows Server 2008
Failover Clustering Tools	Failover Clustering Tools include: • Failover Cluster Manager • Windows PowerShell tools for managing Failover Clustering • The Cluster.exe command-line tool	Not available	√
File Services Tools	File Services Tools include: • Distributed File System Tools, including the DFS Management snap-in, and the Dfsradmin.exe, Dfsrdiag.exe, Dfscmd.exe, Dfsdiag.exe, and Dfsutil.exe command-line tools. • File Server Resource Manager tools, including the File Server Resource Manager snap-in, and the Dirquota.exe, Filescrn.exe, and Storrept.exe command-line tools. • Share and Storage Management Tools, including the Share and Storage Management snap-in.	Not available	√
Group Policy Management Tools	Group Policy Management Tools include: • Group Policy Management Console • Group Policy Management Editor • Group Policy Starter GPO Editor	√	√
Hyper-V Tools	Hyper-V Tools include the Hyper-V Manager snap-in, and the Virtual Machine Connection remote access tool.	Not available	√
Network Load-Balancing Tools	Network Load-Balancing Tools include: • The Network Load-Balancing Manager snap-in • Windows PowerShell tools for managing Network Load Balancing • The Nlb.exe and Wlbs.exe command-line tools	√	√
Remote Desktop Services Tools	Remote Desktop Services Tools include the Remote Desktop Services Manager, and Remote Desktop snap-ins.	√	√

Remote Server Administration Tools technology	Description	Manages technology on Windows Server 2003	Manages technology on Windows Server 2008
Server Manager	Server Manager includes the Server Manager console. Remote management with Server Manager is available only in Windows Server 2008 R2.	Not available	Not available
SMTP Server Tools	Simple Mail Transfer Protocol (SMTP) Server Tools include the SMTP snap-in.	√	√
Storage Explorer Tools	Storage Explorer Tools include the Storage Explorer snap-in.	Not available	√
Storage Manager for Storage Area Networks (SANs) Tools	Storage Manager for SANs Tools includes: • The Storage Manager for SANs snap-in • The Provisionstorage.exe command-line tool	√ Storage Manager for SANs is available in Windows Server 2003 R2 and later versions.	√
Windows System Resource Manager Tools	Windows System Resource Manager Tools include: • The Windows System Resource Manager snap-in • The Wsrmc.exe command-line tool	Not available	√

802.1x user authentication fails when an RDS connection comes in

Article • 09/23/2021 • 2 minutes to read

This article helps fix an issue that occurs when end user uses remote desktop connection to log on to a 802.1x secured Windows 7, Windows 8 or Windows 10 machine that is configured user authentication only.

Applies to: Windows 7 Service Pack 1, Windows 8, Windows 10
Original KB number: 2820847

Symptoms

End user uses remote desktop connection to log on to a 802.1x secured Windows 7, Windows 8 or Windows 10 machine that is configured user authentication only. After about one minute, the connection is lost, and the user are unable to re-establish the remote connection. A local (console) logon may resolve the issue.

Cause

When 802.1x authentication mode is configured to user authentication, the supplicant fails to query the user token in the remote desktop session.

Resolution

To make remote desktop connection works with 802.1x authentication, we must use computer authentication or "User or computer authentication"

Local computer behaves as if the Windows logo key is pressed after you switch from a Remote Desktop session

Article • 12/06/2021 • 2 minutes to read

This article provides a workaround for an issue where your local computer behaves as if you are always pressing and holding the Windows logo key after you start a Remote Desktop Protocol (RDP) session to a remote computer.

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10 - all editions, Windows 7 Service Pack 1
Original KB number: 4467266

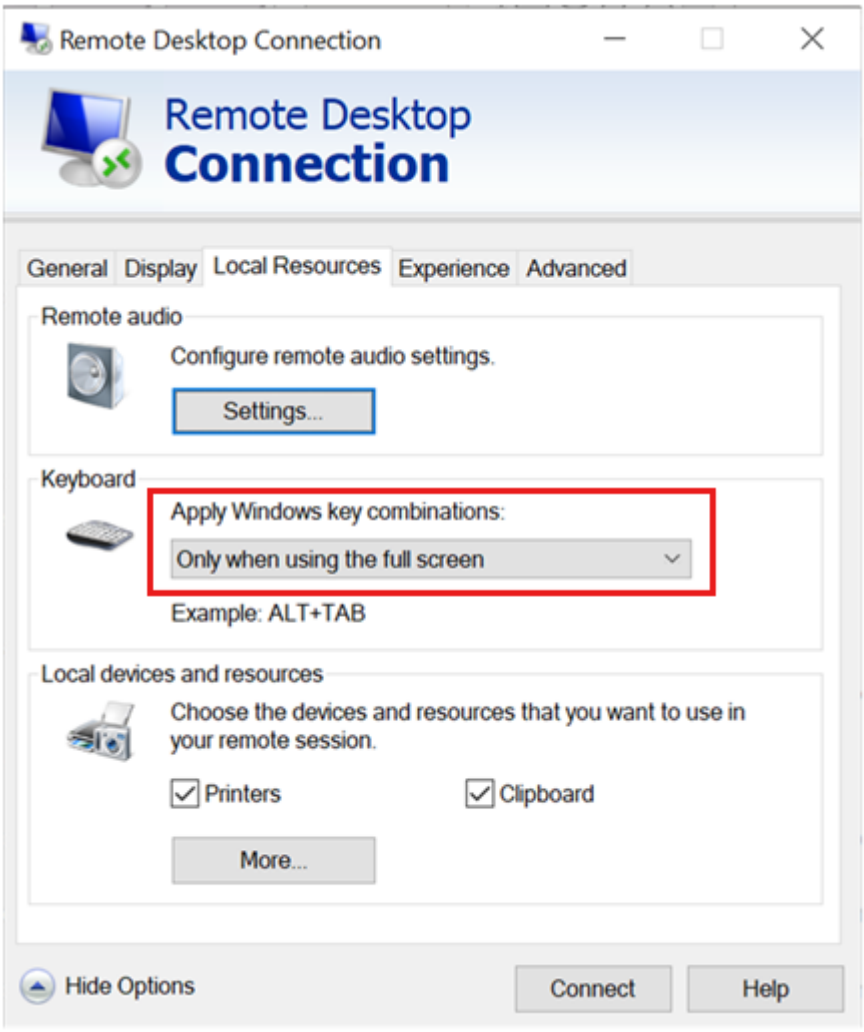
Symptoms

After you start a RDP session to a remote computer, your local computer behaves as if you are always pressing and holding the Windows logo key. For example, when you press the R key, the **Run** box opens. When you press the E key, File Explorer starts.

Cause

This issue occurs if you use particular settings for your Remote Desktop connection and you take the following steps:

1. Before you connect to the remote computer, open the **Local Resources** tab of the **Remote Desktop Connection** dialog box, and set **Apply Windows key combinations** to either **On the remote computer** or **Only when using the full screen**.



2. To start the Remote Desktop session, select **Connect**.

3. If you selected **Only when using the full screen** in step 1, expand the Remote Desktop session window to full screen. If you selected **On the remote computer**, go to step 4.

4. Do the following key sequence:
   a. Press and hold the L key.
   b. Press and hold the Windows logo key.
   c. Release the L key.
   d. Release the Windows logo key.

5. Disconnect the Remote Desktop session, or switch from the Remote Desktop session window to a window on the local computer.

Workaround

To work around this issue, press and release the Windows logo key again after you return to the local computer.

Use Remote Desktop Connection or universal Remote Desktop client instead of RDMan in Windows 10

Article • 02/09/2022 • 2 minutes to read

Virtualization and remote desktops are an important part of your infrastructure and work. And, we recommend that you use Windows built-in Remote Desktop Connection (%windir%\system32\mstsc.exe) or universal Remote Desktop client instead of Remote Desktop Connection Manager (RDCMan).

Applies to: Windows 10 - all editions
Original KB number: 4512838

More information

We're increasing our investments in virtualization and remote desktops, such as Azure Virtual Desktop and RDS on Microsoft Azure.

RDCMan is a client that is widely used to manage multiple remote desktop connections because it's a convenient option. However, RDCMan has not kept pace with the level of advanced technology that we're pursuing.

Instead, we have two great supported client options: Remote Desktop Connection and Universal Client for Windows 10. These clients offer increased security, and they are a key part of our engineering roadmap moving forward. In the future, you can expect even more capabilities, such as the ability to better manage multiple connections.

Some USB devices are not available through RemoteFX USB redirection

Article • 09/23/2021 • 3 minutes to read

This article describes why specific USB devices aren't available for RemoteFX USB redirection, and how to make them available.

Applies to: Windows 7 Service Pack 1
Original KB number: 2653326

Symptoms

On a system where RemoteFX USB redirection is enabled, devices of the following types may not be listed in Remote Desktop Connection under the **Other Supported RemoteFX USB devices** category:

- Printer
- Audio Recording/Playback
- Mass Storage Device (examples include hard drives, CD/DVD-RW drives, flash drives, and memory card readers)
- Smart Card Reader
- PTP Camera
- MTP Media Player
- Apple iPod/iPod Touch/iPhone/iPad
- Blackberry PDA
- Windows Mobile PDA
- Network Adapter

Additionally, composite devices that contain a device interface that corresponds to any of these device types also may not be listed in Remote Desktop Connection under the **Other Supported RemoteFX USB devices** category.

Cause

By default, devices in the categories that are mentioned in the "Symptoms" section are accessible in the remote session by using high-level device redirection methods. These methods of redirection enable optimal performance and backward compatibility of the device in the majority of user scenarios. Therefore, these devices are not offered through RemoteFX USB redirection.

Resolution

An override mechanism is provided to selectively enable the use of specific device types in the categories that are mentioned in the "Symptoms" section through RemoteFX USB redirection. Device types that are enabled by this mechanism will be made available for RemoteFX USB redirection and will appear in Remote Desktop Connection under the **Other Supported RemoteFX USB devices** category. In order to use the device through RemoteFX USB redirection, the device must be selected for remote access by using the Remote Desktop Connection UI, the "usbdevicestoredirect:s: RDP file string, or another method.

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base: 322756 How to back up and restore the registry in Windows
> To enable a device type for RemoteFX USB redirection, follow these steps:

1. Delete all instances of USB storage devices from the client.
2. Make sure that USB storage devices can't be installed on the client through Group Policy.
3. Identify the appropriate interface class GUID for the device type that you want to make available. Examples are as follows:

Device type	Interface class GUID
Hard Drive	{53F5630 7 -B6BF-11D0-94F2-00A0C91EFB8B}
CD-ROM	{53F5630 8 -B6BF-11D0-94F2-00A0C91EFB8B}

For a complete listing of all system-defined device interface classes, please go to the following Microsoft Developer Network website: System-Defined Device Interface Classes

> **Note**

For a device that has multiple interface class GUIDs that are to be made available through this mechanism, only one corresponding interface class GUID has to be added to the registry.

> **Important**
>
> The addition of the following GUIDs is not supported:
>
> - GUID_CLASS_USB_DEVICE
> - GUID_CLASS_USB_HOST_CONTROLLER
> - GUID_CLASS_USBHUB
> - GUID_DEVINTERFACE_USB_DEVICE
> - GUID_DEVINTERFACE_USB_HOST_CONTROLLER
> - GUID_DEVINTERFACE_USB_HUB

4. Locate the following key in the registry of the *client* computer (that is, the computer that is using the Remote Desktop Connection application to connect to another computer):

   `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbSelectDeviceByInterfaces`

   Under this key, use the following format to add a value for each device interface class GUID that you wish to make available:

   Type: REG_SZ (String) Name: Any unique string Data: The interface class GUID, in the following format: {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}, where each x represents a hexadecimal digit, case insensitive. Example To enable RemoteFX USB redirection of CD-ROM drives, add the following value:

   Type: REG_SZ Name: 100 Data: {53F56308-B6BF-11D0-94F2-00A0C91EFB8B}

   Or run the following command from an Administrator command prompt:

   ```
   reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\Client\UsbSelectDeviceByInterfaces" /v 100 /t REG_SZ /d {53f56308-b6bf-11d0-94f2-00a0c91efb8b} /f
   ```

5. Restart Remote Desktop Connection if it is currently running.

More information

For step-by-step instructions on configuring an evaluation deployment of RemoteFX USB redirection for Windows 7 SP1, go to the following Microsoft Technet website:
Configuring USB Device Redirection with Microsoft RemoteFX Step-by-Step Guide

For more information about RemoteFX USB redirection, review the following article on the Remote Desktop Services Blog:
Introducing Microsoft RemoteFX USB Redirection: Part 3

Invalid client IP address in security event ID 4624 in Windows 7 and Windows Server 2008 R2

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution to an issue where event 4624 and an invalid client IP address and port number are generated when a client computer tries to access a host computer that's running RDP 8.0.

Applies to: Windows Server 2008 R2 Service Pack 1, Windows 7 Service Pack 1
Original KB number: 3097467

Symptoms

Assume that the Remote Desktop Protocol (RDP) 8.0 update for Windows 7 and Windows Server 2008 R2 (KB2592687) is installed and enabled through policy settings. When a user's remote desktop logs on to that computer, security event ID 4624 is logged and shows an invalid client IP address and port number, as follows:

> Log Name: Security
> Source: Microsoft-Windows-Security-Auditing
> Date: 9/14/2015 6:10:36 PM
> Event ID: 4624
> Task Category: Logon
> Level: Information
> Keywords: Audit SuccessUser: N/A
> Computer: <computerFQDN>
> Description:
> An account was successfully logged on.
>
> Subject:
> Security ID: SYSTEM
> Account Name: < MachineName>$
> Account Domain: <DomainName>
> Logon ID: 0x3e7
>
> Logon Type: 10

New Logon: Security ID: < DomainName>\<username>
Account Name: < UserName>
Account Domain: <DomainName>
Logon ID: 0x35137
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0x7cc
Process Name: C:\Windows\System32\winlogon.exe

Network Information:
Workstation Name:<computername>
Source Network Address: 244.230.0.0
Source Port: 0

Detailed Authentication Information:
Logon Process: User32
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.
The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The authentication information fields provide detailed information about this specific logon request.

- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.
- Transited services indicate which intermediate services have participated in this logon request.
- Package name indicates which sub-protocol was used among the NTLM protocols.

> - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Cause

This issue occurs because of a code change in RDP 8.0. In RDP 8.0, the client IP address is stored in a WTS_SOCKADDR structure. This differs from RDP 7.0 (the default RDP version in Windows 7 and Windows Server 2008 R2).

In Windows 8 and Windows Server 2012 (and later versions of Windows), the code logic for logging this event is rewritten based on the new design. That prevents this issue from occurring.

Resolution

To resolve this issue, upgrade the RDP target computer to Windows 8 or Windows Server 2012 (or later). Or, disable RDP 8.0 in Windows 7 or Windows Server 2008 R2.

More information

You may also encounter this issue if you're using a third-party RDP component to log on to Windows 7 or Windows Server 2008 R2 when that third-party component uses the same WTS_SOCKADDR structure. In this situation, consider upgrading the OS, or contact the component provider for assistance.

Troubleshooting RDP Client connection problems

Article • 09/23/2021 • 2 minutes to read

This article describes various symptoms for Remote Desktop Client connection failures.

Applies to: Windows Server 2012 R2
Original KB number: 186645

Summary

This article summarizes the various causes for Terminal Server Client connection failures.

More information

Terminal Server Client (Remote Desktop Client) connection failures such as "Unable to RDP, "Remote Desktop Disconnected," or "Unable to Connect to Remote Desktop (Terminal server)" are common problems that we have seen in product support. This article summarizes the various causes for such failures.

The following are some of the commonly seen symptoms:

- You may be limited in the number of users who can connect simultaneously to a Remote Desktop session or Remote Desktop Services session.
- You may have a port assignment conflict.
- You may have an incorrectly configured Authentication and Encryption setting.
- You may have a certificate corruption.

All the steps are documented in these articles, based on the server operating system:

- Server 2003: Remote Desktop disconnected or can't connect to remote computer or Remote Desktop server (Terminal Server) that is running Windows Server 2003
- Server 2008: General Remote Desktop connection troubleshooting
- Server 2008 R2: Troubleshoot "Remote desktop disconnected" errors in Windows Server 2008 R2

Additionally, we have more symptoms documented in the following Microsoft TechNet article:

Troubleshooting General Remote Desktop Error messages

Support policy for Azure Virtual Desktop and Windows 10 Enterprise multi-session

Article • 09/23/2021 • 2 minutes to read

This article describes the support policy for Azure Virtual Desktop and Windows 10 Enterprise multi-session.

Applies to: Windows 10 - all editions
Original KB number: 4491323

Summary

Azure Virtual Desktop

Azure Virtual Desktop (AVD) is now generally available. AVD is a managed desktop and application virtualization service that's hosted on Microsoft Azure. AVD helps deliver the best virtual desktop experience by providing remote access to modern desktop and applications from any device. Combined with Microsoft 365 and Azure, it offers users a multi-session Windows 10 and Microsoft 365 Apps for enterprise environment. Azure Virtual Desktop offers users a more secure computing experience that has improved scalability and reduced IT costs.

Windows 10 Enterprise multi-session

Windows 10 Enterprise multi-session provides multi-session functionality exclusively for Azure Virtual Desktop.

Windows 10 Enterprise multi-session is tested, optimized for, and supported exclusively on Azure. Microsoft does not support Windows 10 Enterprise multi-session on non-Azure deployments (for example, on-premises deployments).

For more information about Azure Virtual Desktop and Windows 10 Enterprise multi-session, see Azure Virtual Desktop.

Shell Experience troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Shell Experience-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Shell Experience sub categories

- Cortana and Search
- Desktop Shell
- DPI and Display Issues
- DST and Timezones
- File Associations
- File Explorer/Windows Explorer
- Lock Screen or Screensaver
- Modern, Inbox and Microsoft Store Apps
- Windows Media Player
- Windows Search

Windows Search service not starting with Windows Search service on local computer started and then stopped error

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution to solve the error that occurs when you try to start the Windows Search Service.

Applies to: Windows 10 - all editions
Original KB number: 2484025

Symptoms

Windows Search service doesn't start and when you try to start the service manually, you receive this error message:

> ========
> Services
> ========
> "The Windows Search service on local computer started and then stopped. Some services stop automatically if they are not in use by other services or programs"
> ===
> OK
> ===

Cause

You may see this issue if there are missing subkeys or registry entries under the following registry location:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Search\CrawlScopeManager\Windows\SystemIndex`

Or if there are corrupted log files at the following location:

C:\windows\system32\config\TxR

> ⓘ **Note**
>
> The above regisrty key is unique to each machine, so should not be replaced manually.

Resolution

To resolve this issue, delete all files with `.BLF` and `.REGTRANS-MS` extension in the following directory:

C:\windows\system32\config\TxR

> ⓘ **Note**
>
> The files in the folder location above are hidden and will thus not be visible unless you set the system to not Hide Protected Operating System Files under **Tools** > **Folder Options**.

Once these files are deleted, reboot the machine. Once rebooted, observe that the Windows Search service has already started and is in process of rebuilding the Index.

> ⓘ **Important**

You may observe High CPU while the Search Index is being rebuilt.

Fix problems in Windows Search

Article • 12/30/2022 • 4 minutes to read

Try our Virtual Agent - It can help you quickly identify and fix common Windows Search issues.

If Windows Search is unresponsive or the search results don't appear as expected, try any of the following solutions in this article.

Original KB number: 4520146

Solution 1: Check for updates

Windows 11 and Windows 10 let you choose when and how to get the latest updates to keep your device running smoothly and securely. To manage your options and see any available updates, select the **Start** button, and then go to **Settings** > **Update & Security** > **Windows Update** > **Check for updates**. Install any available updates, and then restart your computer if the updates require it.

For more information, see Update Windows.

Solution 2: Search and Indexing troubleshooter

Your PC automatically indexes content to deliver faster search results. If you're running Windows 10, version 1903 (May 2019 Update) or later versions and Windows can detect a problem, we'll run the Search troubleshooter automatically. This troubleshooter will reset Windows Search back to the default experience. View your troubleshooter history under **Settings** > **Update & Security** > **Troubleshoot** > **View History**. Follow the solutions below if your issue is still not resolved.

Use the Windows **Search and Indexing** troubleshooter to try to fix any problems that may arise. To use the troubleshooter, follow these steps:

1. Select **Start** > **Settings**.
2. In **Windows Settings**, select **Update & Security** > **Troubleshoot**. Under **Find and fix other problems**, select **Search and Indexing**.
3. Run the troubleshooter and select any problems that apply. Windows will try to detect and solve them.

You can also use a command prompt to open the troubleshooter. Press the Windows logo key+R, enter *cmd* in the **Open** box, and then select **OK**. At the command prompt,

run the following command:

```
Console

msdt.exe -ep WindowsHelp id SearchDiagnostic
```

For more information about Search and Indexing, see the following articles:

- Performance issues that affect Windows Search and Search indexing.
- FAQs on Search indexing in Windows 10.

Solution 3: Restart Windows Search

End the **SearchUI** process to restart Windows Search by following these steps:

1. Press `Ctrl`+`Alt`+`Delete`, and then select **Task Manager**.
2. In the **Task Manager** window, select the **Details** tab.
3. In the **Name** column, right-click **SearchUI.exe**, and then select **End task**.
4. When you're prompted to end *SearchUI.exe*, select **End process**.

> **Note**
>
> The Windows Search process will automatically restart the next time you search.

If this solution doesn't fix your problem, try restarting your device. Restarting will also install any pending updates.

> **Note**
>
> You may want to bookmark this page before you restart.

Solution 4: Reset Windows Search

Try resetting Windows Search by using the method that's appropriate for your version of Windows.

To determine which version of Windows your device is running, follow these steps:

1. Select **Start** > **Settings** > **System** > **About**.

2. Under **Windows specifications**, check which version of Windows your device is running.

> **Note**
>
> Resetting Windows Search doesn't affect your files. However, it may temporarily affect the relevance of search results.

Windows 10, version 1809 and earlier

If the Windows 10 October 2018 Update or an earlier update is installed, reset Cortana to reset Windows Search by following these steps:

1. Select **Start**, right-click **Cortana**, and then select **More** > **App settings**.
2. In the Cortana settings, select **Reset**.

Windows 11, Windows 10, version 1903, and later

If Windows 11, Windows 10 May 2019 Update, or a later update is installed, use Windows PowerShell to reset Windows Search by following these steps:

> **Important**
>
> You must have administrator permissions to run this script.

1. Download the *ResetWindowsSearchBox.ps1* script from the Reset Windows Search PowerShell script, and save the file to a local folder.
2. Right-click the file that you saved and select **Run with PowerShell**.
3. If you're asked the following question, select **Yes**.

   > Do you want to allow this app to make changes to your device?

4. The PowerShell script resets the Windows Search feature. When the word **Done** appears, close the PowerShell window.
5. If you receive the "Cannot be loaded because running scripts is disabled on this system" error message, enter the following command on the command line of the PowerShell window, and then press Enter:

   ```
   
   ```

PowerShell

```
Get-ExecutionPolicy
```

> **Note**
>
> The current policy appears in the window. For example, you might see **Restricted**. We recommend that you note this value because you'll have to use it later.

6. Enter the following command on the command line of the PowerShell window, and then press Enter:

PowerShell

```
Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted
```

> **Important**
>
> You'll receive a warning message that explains the security risks of an execution policy change. Press Y, and then press Enter to accept the change.

To learn more about PowerShell execution policies, see About Execution Policies.

7. After the policy change is completed, close the window, and then repeat steps 2-4. However, when the **Done** message appears this time, DON'T close the PowerShell window. Instead, press any key to continue.

8. Revert to your previous PowerShell execution policy setting. Enter the following command on the command line of the PowerShell window, press the Spacebar, enter the policy value that you noted in step 5, and then press Enter:

PowerShell

```
Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy
```

For example, if the policy that you noted in step 5 was **Restricted**, the command would resemble the following one:

PowerShell

```
Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted
```

> **Note**
>
> You'll receive a warning message that explains the security risks of an execution policy change. Press Y, and then press Enter to accept the change and revert to your previous policy setting.

9. Close the PowerShell window.

> **Important**
>
> If your organization has disabled the ability to run scripts, contact your administrator for help.

Help us improve Search in Windows

If the previous suggestions don't fix the problem, let us know by sending feedback in the Feedback Hub. Provide details, such as a description of the problem, screenshots, log files, and any other information that might be helpful. In the Feedback Hub, select the appropriate category and subcategory. In this case, submit your feedback in the **Cortana and Search** category.

Known issues for Windows Desktop Search and Cortana in Windows 10

Article • 09/23/2021 • 2 minutes to read

This article describes the known issues that may occur when you use Windows Desktop Search or Cortana in Windows 10.

> **Note**
>
> Home users: This article is intended for use by support agents and IT professionals. If you're looking for more information about website error messages, please see the following Windows website: **Search for anything, anywhere**

Applies to: Windows 10 - all editions
Original KB number: 3206883

Known issues

Issue 1

Desktop Search or Cortana can't find shortcut files (.lnk)

Symptoms

On a computer that's running Windows 10, Desktop Search, or Cortana, you can't find shortcut files (files with an LNK extension).

The issue occurs regardless of whether the shortcut files are in indexed locations.

Status

Microsoft is aware of this issue and is investigating it.

Issue 2

Desktop Search or Cortana don't find files that have a URL extension.

Symptoms

On a computer that's running Windows 10, you can't find files that have a URL extension by using Desktop Search or Cortana.

Status

This is by design. The search filters the results to eliminate noise that's caused by non-app shortcuts.

Issue 3

Windows Desktop Search shows no results if you have your **Internet Options** settings configured to disable website data.

Symptoms

When you try to search from the **Start** menu or from Cortana on a Windows 10-based computer, you receive no results. This behavior occurs if you have your **Internet Options** settings configured to disable local caches and databases.

You can disable local caches and databases by using one of the following methods:

- Using Internet Explorer: **Internet Options** -> **General** tab -> **Browsing History** -> **Settings** -> **Website Data Settings** -> **Caches and databases** tab -> **Allow website caches and databases** (clearing the check box)
- Using Registry Editor:
  `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\BrowserStorage\AppCache` "AllowWebsiteCaches"=dword:00000000
- Using Group Policy:
  Group Policy under either or both User and Computer configuration:

  Administrative Templates>Windows Components> Internet Explorer>Internet Control Panel>General Page>Browsing History>Allow websites to store application caches on client computers

Cause

This issue occurs when the user disables the use of caches and databases through Internet Options or Group Policy. Doing this prevents the application that uses AppCache from storing data locally, and the application must have access to the web content that would have been used initially to populate the cache. If a computer has no

Internet access and has the option configured to disallow the Web Platform APIs from using AppCache (The **Allow website caches and databases** option is cleared), Desktop Search doesn't work.

Resolution

To work around this problem, change the configuration of Desktop Search through Group Policy. To do this, follow these steps:

1. Press the Windows key + R to open the **Run** box.
2. Type *gpedit.msc*, and then press **Enter**.
3. In the Group Policy Editor, navigate to the following location:

   Computer Configuration -> **Administrative Templates** -> **Windows Components** -> **Search**
4. In the pane on the right, double-click. Don't search the web or display web results in Search.
5. Select Enabled.
6. Click **Apply**, and then click OK. Desktop Search will now avoid using any of the Web Platform APIs to acquire content from the web. This also mitigates the impact of disabling website caching and databases.

More information

Windows Desktop Search, Internet Explorer, and Microsoft Store Apps use a feature called Application Cache (AppCache), which enables the creation of offline web apps and webpage caching. AppCache also lets the apps that use it boost performance of web content by reducing the number of requests made to the hosting server.

Troubleshoot Windows Search performance

Article • 10/28/2022 • 8 minutes to read

Try our Virtual Agent - It can help you quickly identify and fix common Windows Search issues.

This article provides guidelines for troubleshooting poor Windows Search performance.

Applies to: Windows 10 – all editions
Original KB number: 4558579

Summary

This article discusses common performance issues that affect Windows Search and Search indexing.

If you observe general poor performance when you search or when Windows builds a search index, go to Tune the Indexer performance.

If you observe specific error messages, go to Troubleshoot Search errors.

More information

Tune the Indexer performance

The primary factors that affect indexing performance are the number of items indexed and the overall size of the index. These factors are related but separate.

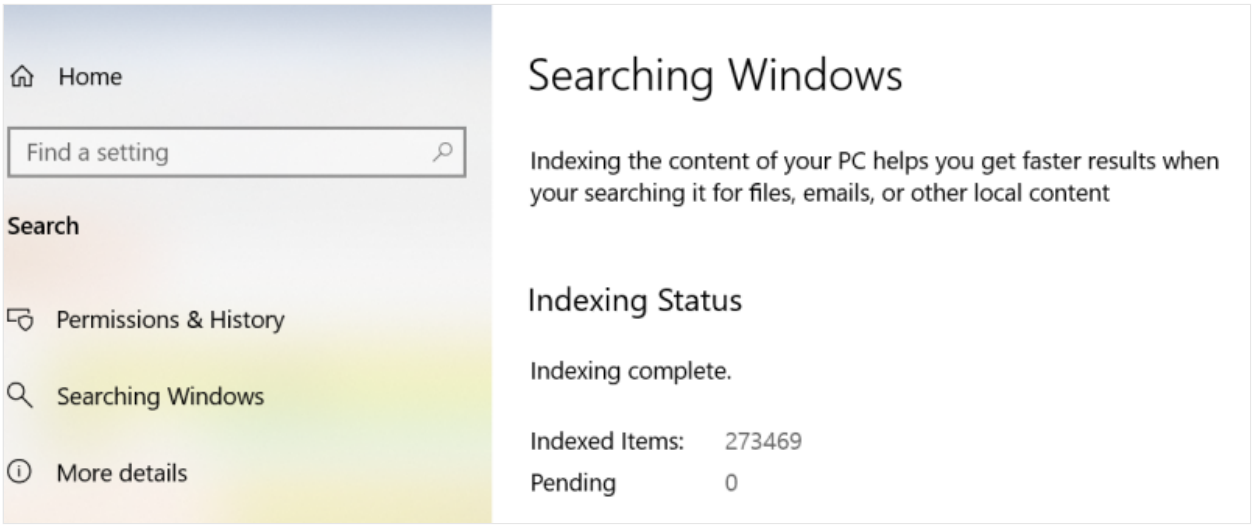
Number of items indexed

On a typical user's computer, the Indexer indexes fewer than 30,000 items. On a power user's computer, the Indexer might index up to 300,000 items. If the Indexer indexes more than 400,000 items, you may begin to see performance issues. For more information, go to Size of the index database.

The Indexer can index up to 1 million items. If the Indexer tries to index beyond that limit, it may fail or cause resource problems on the computer (such as high usage of CPU, memory, or disk space).

> **Note**
>
> By default, the Indexer indexes any Outlook mailboxes on the computer. If a mailbox contains more than 6 million items, the performance of the Indexer may degrade. For more information, go to the "Change Outlook settings" section.

To check the number of indexed items, select **Settings** > **Search** > **Searching Windows**, and then check the value of **Indexed items**.



Size of the index database

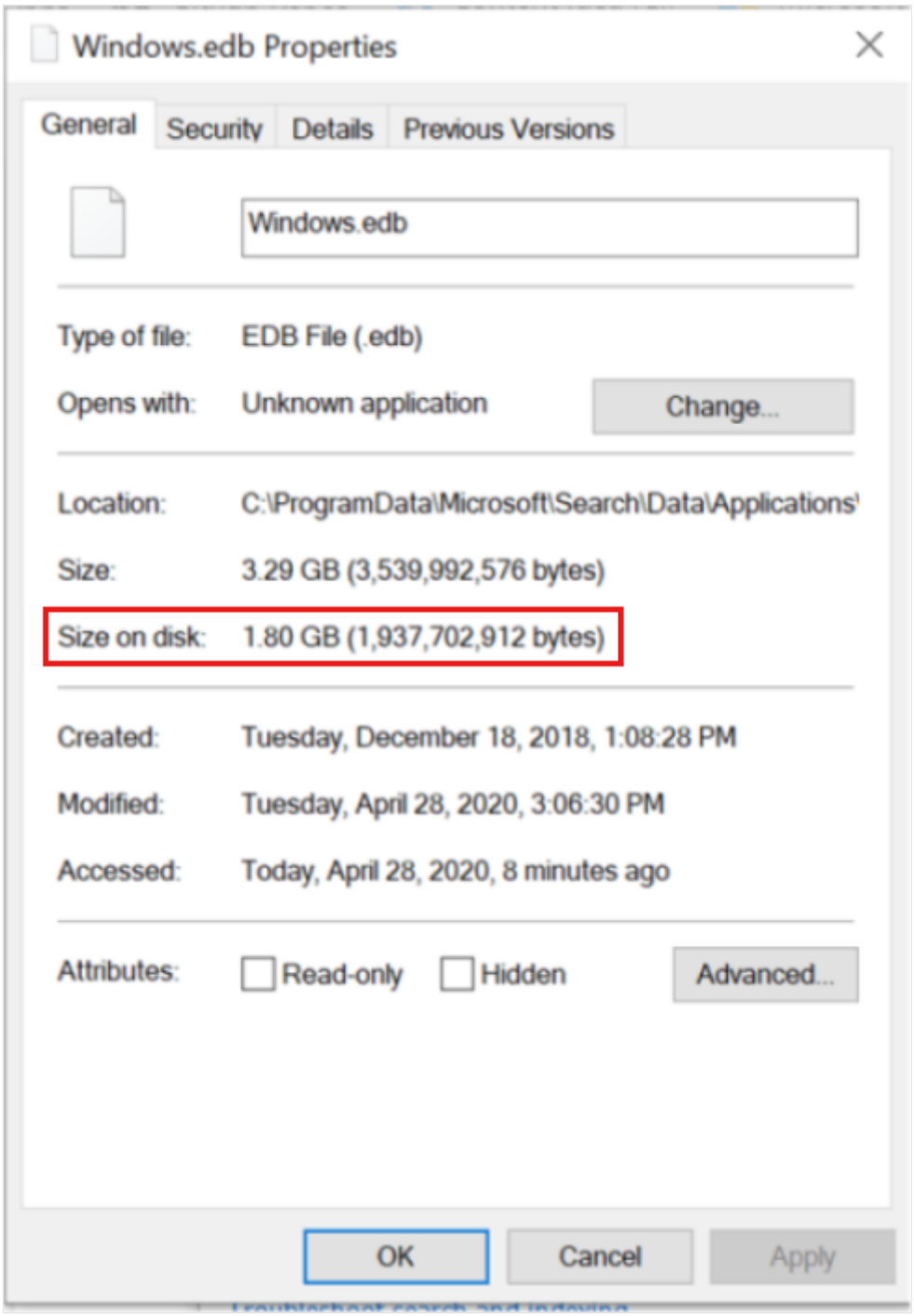
As the number of indexed items grows beyond 400,000, the index database grows considerably regardless of the size of those items. The size of the items also affects database size. A database that contains either a few large files or a large number of smaller files can affect performance. Both factors together can compound the problem. The Indexer tries to compress the index data. However, this approach becomes less effective as the index database grows.

> **Important**
>
> To check the size of the index database, use the **Size on disk** property of the Windows.edb file instead of relying on the **Size** property or the file size that's listed in Explorer. Because of the compression algorithms that the Indexer uses on sparse ESE and NTFS files, the value that's listed in Explorer may not be accurate. Additionally, this **Size** value might include space that was used by or allocated to the file in the past, instead of using the current size.

By default, Windows.edb is located in the C:\ProgramData\Microsoft\Search\Data\Applications\Windows folder. To check the size

of the file, follow these steps:

1. Right-click Windows.edb, and select **Properties**.
2. Check the **Size on disk** value. This property reflects the actual disk space that the database uses.



Tuning methods

You can use any of several approaches to improve the performance of Search and the Search Indexer.

> **Important**

To make sure that the index reflects your changes, select **Settings** > **Search** > **Searching Windows** > **Advanced Search Indexer Settings** > **Advanced** > **Rebuild**.

Let the Indexer run for up to 24 hours to rebuild the index database.

Exclude folders

You can use this approach to reduce the number of items that are indexed and to reduce the size of the index database. To exclude whole folders from the index, select **Settings** > **Search** > **Searching Windows** > **Add an excluded folder**. And then select a folder to exclude.

For a more granular method to include or exclude items, open **Searching Windows**, and select **Advanced Search Indexer Settings**. In **Indexing Options**, select **Modify**, and then select or deselect locations to index.

Change how the Indexer treats specific file types

To control how the indexer treats specific file types, open **Indexing Options**, and select **Advanced** > **File Types**. You can change how the Indexer treats specific file types (identified by file extension) or add and configure new file types.

Defragment the index database

You can use this approach to reclaim empty space within the index database. Open an administrative Command Prompt window, and then run the following commands in the given order:

```
Console

Sc config wsearch start=disabled
Net stop wsearch
EsentUtl.exe /d
%AllUsersProfile%\Microsoft\Search\Data\Applications\Windows\Windows.edb
Sc config wsearch start=delayed-auto
Net start wsearch
```

For more information about how to defragment the index database, see the following Knowledge Base article:

2952967 Windows.edb larger than expected when a PST file is indexed in Windows

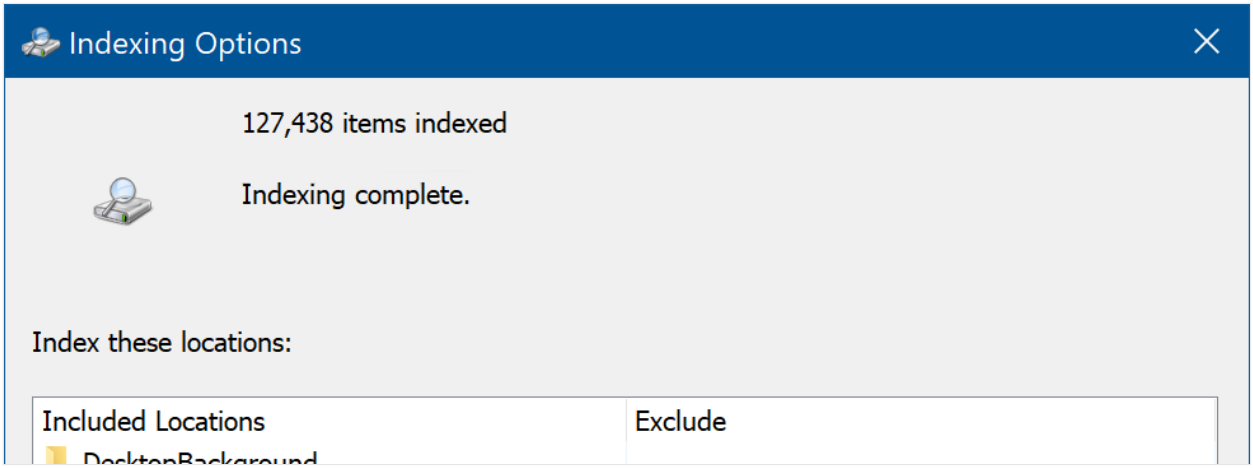
Change Outlook settings

To help reduce the content of an Outlook mailbox, you can change the synchronization window to a shorter time interval than the default interval of one year. For more information, see the following article:

3115009 Update allows administrators to set additional default mail and calendar synchronization windows for new Exchange accounts in Outlook 2016

Troubleshoot Search errors

If the Indexer successfully builds the index database, you see the message **Indexing complete** on the Windows Search settings page and in **Indexing Options**.



If a different message appears, see the following table for more information about the message and how to respond.

Status message	Explanation	Possible actions
Indexing complete	The Indexer is running as usual, and has finished indexing.	Indexing should be complete, and all results available. If you're still missing files, make sure that the correct folders are selected to search. To see a detailed list of the locations that are indexed, open **Searching Windows**, and select **Advanced Search Indexer Settings**. In **Indexing Options**, select **Modify**.

Status message	Explanation	Possible actions
Indexing in progress. Search results might not be complete during this time.	The Indexer has found new files on the system and is adding them to the index. Depending on the number of files that have recently changed, it could take a few hours	Leave the computer turned on and connected to power (if applicable) for a few hours to let indexing finish.
Indexing speed is reduced because of user activity.	The Indexer is adding new items to be searched, but has slowed its progress because the user is interacting with the device.	The indexing process will complete slowly. Wait a few hours, or leave the device unattended and connected to a power source.
Indexing is waiting for computer to become idle.	The Indexer has detected items that have to be indexed, but the device is too busy for the indexing process to continue.	Find out what is causing device to be busy. If the disk or CPU use is high, the indexer stops running to maximize the resources for foreground activities.
Indexing is paused to conserve battery power.	The Indexer has stopped adding new items to the index because of low battery power. Search results may not be complete.	Connect the device to power, and charge the battery. After the battery has sufficiently charged, indexing resumes.
Your group policy is set to pause indexing while on battery power.	Your IT department has configured the Indexer pause while the device uses battery power.	To finish indexing, connect the device to power. Contact your IT team if you want to change the policy.
Indexing is paused.	The Indexer has been paused from the Windows Search settings page.	Indexing resumes 15 minutes after it pauses. To resume indexing more quickly, restart the Windows Search service (`wsearch`). You can do it by using the **Services** tab of Task Manager or by using Services.msc.

Status message	Explanation	Possible actions
Indexing is not running.	Indexer hasn't started or is disabled.	If you have upgraded Windows on the device, wait five minutes for the Windows Search service to start. The service automatically pauses during an upgrade. The service should have the following configuration: - **Status**: Running - **Startup Type**: Automatic (Delayed Start) Otherwise, make sure that the Windows Search service (`wsearch`) is configured correctly. To do this, open Services.msc, and scroll to the Windows Search service. To change the Windows Search service settings, right-click **Windows Search**, and then select **Properties**. Some anti-virus programs and "Optimize your PC" applications disable the Windows Search service. We recommend that you don't run such applications if you want to use Search. Or, check the status of the service after you run the applications.
Insufficient memory to continue indexing. Search results might not be complete.	The Indexer detected a low memory state and stopped to preserve the user experience.	Use Task Manager to discover applications that use a large amount of memory. If possible, close those applications. Install more memory in the device.
Insufficient disk space to continue indexing. Search results might not be complete.	There's not enough space on the disk to continue indexing. The Indexer stops before it fills the entire disk. The index is generally 10 percent of the size of the content that is being indexed.	Make sure that there's more than 1 GB of free space on the disk. Reduce the size of the database index, as described in this article.
Waiting the receive indexing status...	The Indexer hasn't replied to the status query.	Wait for the Indexer to reply. It should take about one minute. In Task manager, confirm that the searchindexer.exe process is running.
Indexing is starting up.	The Indexer is starting.	Wait for the Indexer to start. It should take about one minute.

Status message	Explanation	Possible actions
Indexing is shutting down.	The Indexer has received the signal to shut down either because the operating system is shutting down or because the user requested it.	Make sure that the user hasn't manually stopped the service. Check the status of the Windows Search Service (`wsearch`) in services.msc.
Index is performing maintenance. Please wait.	The Indexer is trying to recover and optimize the index database. It could occur because lots of content was added recently, or because the Indexer encountered a problem while writing out data to the hard disk.	Wait a few minutes for the Indexer to finish. It can take up to 30 minutes on a slow computer. Make sure that the system hard disk isn't generating failures. Usually, Indexer writing issues precede drive failure. Make sure that the user has backed up personal data.
Indexing is paused by an external application.	An application on the computer requested the Indexer to stop. It commonly occurs during Game mode or during an upgrade.	Make sure that the device isn't in Game mode. Use services.msc or Task Manager to restart the Windows Search service. It resumes indexing until the next time that an external app requests a pause.
The status message is missing, and the entire page is greyed out.	Something has corrupted the Indexer registry keys or database. The service can no longer start or report status.	Delete the contents of C:\ProgramData\Microsoft\Search\Data.Refresh the operating system.

Windows.edb is larger than expected when a PST file is indexed

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where Windows.edb becomes larger than expected when PST files are indexed in Windows 10, 8.1, or 8.

Applies to: Windows 10 - all editions
Original KB number: 2952967

Symptoms

When you index a PST file from **Control Panel** > **Indexing options**, the size of the Windows.edb file (which is located under `%ProgramData%\Microsoft\Search\Data\Applications\Windows`) grows in proportion to the size of the PST file. This issue can result in low disk space and other performance issues. This issue doesn't occur in Windows 7.

Cause

There are two reasons why Windows.edb is larger in Windows 8, Windows 8.1 and Windows 10 than in Windows 7:

- Both properties and persistent indexes are stored in Windows.edb starting with Windows 8. in Windows 7, only properties are stored in Windows.edb-p persistent indexes are stored separately, in *.ci files.
- Windows 8, Windows 8.1 and Windows 10 indexes the entire contents of files, regardless of their size. Windows 7 indexes only the first part of large documents.

Neither of these behaviors is configurable on Windows 8, Windows 8.1 or Windows 10. This behavior improves recall for searches and general performance of indexing and querying.

Workaround

To work around this issue, follow these steps:

1. Index less content. If you have a lot of content, Windows.edb can be expected to grow very large. In this case, the only option to reduce disk usage is to index less

content locally (by having Outlook cache less mail locally or by changing scopes in Indexing **Options** > **Modify**, followed by rebuilding the index from **Advanced** > **Rebuild**).

2. Run an offline defrag of the .edb file from a command prompt by running the following commands:

```
Console

Sc config wsearch start=disabled
Net stop wsearch

EsentUtl.exe /d
%AllUsersProfile%\Microsoft\Search\Data\Applications\Windows\Windows.ed
b

Sc config wsearch start=delayed-auto

Net start wsearch
```

Windows 8 and Windows 8.1 app titles have an "x" in the lower-right corner

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where the titles for Windows 8 and Windows 8.1 apps have an "x" in the lower-right corner.

Applies to: Windows 10 - all editions
Original KB number: 2832072

Symptoms

After you boot your computer to the Windows 8 or Windows 8.1 Start screen, you may find that some or all of the Windows 8 and 8.1 app titles have an "x" in the lower-right corner. When you click one of the app titles to start the app, you receive the following message:

> This app can't open
>
> Check the Microsoft Store for more info about <*AppName*>.
> Go to the Store

Cause

This behavior may be caused by an error that occurred when an app package was first installed or injected into the Windows 8 or Windows 8.1 image. Or, it may be caused by out-of-date software.

Resolution

This issue may be resolved by just waiting several minutes, as the issue may be fixed by Windows.

If the issue is not resolved after several minutes, first try checking for Windows updates, as updating Windows may fix the problem. To check for updates, follow these steps:

1. Open Windows Update by swiping in from the right edge of the screen (or, if you're using a mouse, point to the lower-right corner of the screen and move up the mouse pointer), tapping or clicking **Settings**, tapping or clicking **Change PC settings**, and then tapping or clicking **Update and recovery**.

2. Tap or click **Check now**, and then wait while Windows searches for the latest updates for your computer.
3. If updates are found, tap or click **Install updates**.
4. Read and accept the license terms, and then tap or click **Finish** if the update requires it.

If updating Windows does not work, you may be able to resolve this issue by either installing a new app from the Microsoft Store or by reinstalling or updating existing apps. Doing this may update or fix a dependency that multiple apps rely on.

If this does not resolve the issue, you may have to contact the original equipment manufacturer (OEM) that you purchased the computer from. Or, contact Microsoft Support.

More information

If you are the individual or engineer who creates the Windows image, you may want to closely monitor the injection of app packages to look for errors or messages that indicate that there was a failure.

This issue may also occur after you perform a refresh of the system by using the push-button reset features.

Windows 7 black screen on computer unlock

Article • 02/07/2022 • 2 minutes to read

This article provides a solution to an issue where Windows black screen when unlocking a computer.

Applies to: Windows 7 Service Pack 1
Original KB number: 2431700

Symptoms

Consider the following scenario:

1. A Windows Vista or Windows 7 computer is running the "Aero" graphics mode.
2. The Windows Vista or Windows 7 computer is subject to additional security restrictions and security software, such as might be the case in the enterprise, or with mandated security settings and software such as DISA or DoD requirements.
3. The computer is locked and left undisturbed long enough for the screen to go black, which is 20 minutes with the default power policy of "Balanced".
4. A person unlocks the computer by entering their user credentials.

After the credential is entered, the screen goes black, and remains black for as much as 10 minutes or longer. The machine isn't "hard-locked", as periodic disk-drive activity may be noted from the disk-drive indicator light on the computer, if so equipped.

Cause

A problem with some layer of security software causes the Desktop Window Manager to wait for an unspecified amount of time.

Resolution

1. A temporary workaround is to Stop and Disable the "Desktop Window Manager Session Manager" service. Disabling this service will turn off the "Aero" graphics display feature, which will disable certain features such as Aero Peek, Aero Snap, Aero Shake, and so on. To disable this service:
   a. Click the **Start** button, type *services.msc* and then press the ENTER key, or click the icon that comes up under **Programs** in the Instant Search box.

b. Locate and then double-click the Desktop Window Manager Session Manager service.
c. Locate the **Startup type** dropdown and change the value to "disabled".
d. Locate and click the button labeled "Stop".
e. Click the **Apply** button, and then click the **OK** button.

Alternatively, you can run the following commands from an elevated CMD prompt to set the service properties of the Desktop Window Manager Session Manager service to not running and disabled:

```
Console

net stop UxSms
sc config UxSms start= disabled
```

To return the settings for the Desktop Window Manager Session Manager service to normal via the CMD line:

```
Console

sc config UxSms start= auto
net start UxSms
```

2. Updated display drivers may resolve this issue. You can determine the manufacturer of the display adapter by following these steps:
   a. Click **Start**, and in the **Search Programs and Folder** text box, type in *MSINFO32* (without quotation marks) and press ENTER.

      > ⓘ **Note**
      >
      > The System Information tool should appear.

   b. On the left-hand section called **System Summary** locate Components, and under **Components** locate and click on **Display**.
   c. The right-hand section of **System Information** should now display information about the display system in the computer. The item called "Name" should indicate the type of display adapter.
   d. At this point you can go to the Internet web site of the vendor, or the vendor of your computer to locate updated drivers.
   e. In some cases, you may be offered updated video drivers by running Windows Update.
   f. If you are not sure of which drivers to install, contact the vendor of your computer hardware for assistance in locating an updated display driver

package.

3. Another solution is to discover what layer of security software is causing the temporary blocking, which renders the screen black and therefore unusable. That layer of software would need to be uninstalled or updated to prevent the blocking condition in the Desktop Window Manager.

More information

One symptom that has been noted if this condition is true is that the DWM, or Desktop Window Manager process will consume an ever increasing amount of memory, as displayed in Task Manager.

Blank desktop in Windows

Article • 09/23/2021 • 3 minutes to read

This article provides resolutions to an issue where you're presented with a blank screen with no Start Menu, shortcuts, or icons after logging on to a Windows computer.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 970879

Symptoms

After logging on to a Windows computer, you're presented with a blank screen with no Start Menu, shortcuts, or icons. If you reboot and use F8 to boot to Safe Mode with Networking, you'll see your normal desktop.

You may see the following events in the Application log:

> Log Name: Application
> Source: Microsoft-Windows-Winlogon
> Event ID: 4006
> Level: Warning
> User: N/A
> Computer: M1.Contoso.com
> Description:
> The Windows logon process has failed to spawn a user application. Application name: . Command line parameters: C:\Windows\system32\logon.scr /s.
>
> Log Name: Application
> Source: Microsoft-Windows-Winlogon
> Event ID: 4006
> Level: Warning
> User: N/A
> Computer: M1.Contoso.com
> Description:
> The Windows logon process has failed to spawn a user application. Application name: . Command line parameters: C:\Windows\system32\userinit.exe.

Cause

This may occur when the membership of the local Users group is changed from the default settings. By default, the local Users group should contain the Interactive account and the Authenticated Users group.

By default, User Account Control (UAC) is enabled. At logon, the standard user access token is built, and if the Users group is missing the default members, the user will be unable to interact with the desktop, resulting in the blank desktop being displayed.

Resolution

Add the Authenticated Users group and Interactive account to the local Users group.

For both methods below, you'll need to first restart and select F8 at boot to boot to Safe Mode with Networking.

Method 1

1. Click **Start**, **Run**, type *lusrmgr.msc*, and then press ENTER.
2. Select **Groups** in the left pane.
3. Double-click **Users** in the right pane.
4. Click **Add**, and then click **Locations**. Scroll to the top of the Locations dialog and select the local computer name, then click **OK**.
5. In the Enter the object names to select field, type Interactive; Authenticated Users (separated by a semi-colon). Then click **OK**.
6. Restart the computer.

Method 2

Run the following commands from a command prompt:

Console

```
Net localgroup Users Interactive /add
Net localgroup Users "Authenticated Users" /add
```

More information

When an administrator logs on, the full administrator access token is split into two access tokens: a full administrator access token and a standard user access token.

During the logon process, the administrative privileges and user rights in the full administrator access token are filtered, resulting in the standard user access token. The standard user access token is then used to launch the Explorer.exe process that displays the desktop.

When the local Users group doesn't contain the default members, the standard user access token doesn't have sufficient permissions available to launch Explorer.exe, and only a blank desktop is displayed.

When UAC is turned off, only the full privilege access token is generated for the user and the membership of the local Users group doesn't impact the permissions available in that token.

Windows makes a distinction between the built-in Administrator account and members of the Administrators group. The built-in Administrator account still has full read/write access to the computer and runs with the full administrative access token. UAC administrators are also members of the local Administrators group, but they run with the same access token as standard users.

Disclaimer

Microsoft and/or its suppliers make no representations or warranties about the suitability, reliability, or accuracy of the information contained in the documents and related graphics published on this website (the materials) for any purpose. The materials may include technical inaccuracies or typographical errors and may be revised at any time without notice.

To the maximum extent permitted by applicable law, Microsoft and/or its suppliers disclaim and exclude all representations, warranties, and conditions whether express, implied, or statutory, including but not limited to representations, warranties, or conditions of title, non-infringement, satisfactory condition or quality, merchantability and fitness for a particular purpose, with respect to the materials.

Standard user: RunOnce and RunOnceEx are not being executed

Article • 09/23/2021 • 2 minutes to read

This article provides help to fix an issue where standard users can't execute a command set via RunOnce or RunOnceEx.

Applies to: Windows 10 - all editions
Original KB number: 2021405

Symptoms

A command set to execute via RunOnce or RunOnceEx may not execute as expected. The registry keys affected are:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunonceEx`

Cause

This will occur if you log on with a Standard User Account. This is by design.

Resolution

To execute commands from those registry keys, you must log in with an Administrator account. This issue effects only users with a Standard User account. If the user has an Administrator or Split Token, the execution proceeds.

You receive 0x80070005 error when you try to register a DLL by using Regsvr32.exe

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to a 0x80070005 error that occurs when you register a DLL by using Regsvr32.exe.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 827659

Symptoms

When you try to register a dynamic-link library (or DLL, or .dll file) by using the Regsrv32.exe command-line tool, the DLL is not registered, and you may receive the following error message:

> DllRegisterServer in **file_name**.dll failed.
>
> Return code was: 0x80070005

> **Note**
>
> This behavior does not occur in Windows NT 4.0 or Windows 2000.

Cause

This behavior may occur if you try to register a DLL by using Regsrv32 while you are logged on using an account that does not have administrative credentials, such as an account that is a member of the standard users group. An account that does not have administrative credentials cannot write to the registry or change files in the System32 folder.

The behavior occurs because Windows XP and Windows Server 2003 use a more restrictive security scheme than earlier versions of Windows use. This scheme prevents standard users from registering DLLs.

> **Note**
>
> Because of this behavior, standard users may not be able to run programs that self-register DLLs by using standard user's ID.

Resolution

To resolve this behavior, log on by using an administrator account, and then register the DLL.

More information

You can register a DLL by using an account that does not have administrative credentials as long as the DLL does not write to the registry or change files in the System32 folder.

Disabling Autoplay through Group Policy or the registry will cause HotStart buttons to not function

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where HotStart buttons doesn't work when Autoplay is disabled.

Applies to: Windows 7 Service Pack 1
Original KB number: 2328787

Symptoms

Consider the following scenario:

- You have a Windows 7 system running on a laptop with Hotstart buttons
- There is a policy set in Group Policy to disable Autoplay on all drives

In this scenario, the HotStart buttons do not function

Cause

When changing the Group Policy setting to disable Autoplay, the Autoplay registry value gets set to 0xFF (disable Autoplay on all drives). When the registry value is set to 0xFF, HotStart does not function.

Resolution

You can change the settings by using Group Policy settings.

There are three options: "Not Configured", "Enabled", and "Disabled" in the "Turn off Autoplay".

When selecting "Enabled", you need to select "CD-ROM and removable media drives" to allow HotStart to function.

By selecting this option, the Autoplay registry value is set to "0xB5", and fixed and RAM drives are the only ones still enabled. Any other drives: unknown types, removable drives, network drives, and CD-ROM drives are disabled.

How to open Group Policy settings as follows:

1. Click Start, type Gpedit.msc in the Start Search box, and then press ENTER.

   If you are prompted for an administrator password or for confirmation, type the password, or click Allow.

2. Under Computer Configuration, expand Administrative Templates, expand Windows Components, and then click Autoplay Policies.

3. In the Details pane, double-click Turn off Autoplay.

   If you are experiencing this on a system that has been joined to a domain, you will need to contact the domain administrator for assistance. Your system settings synchronize to the domain server.

   For operating systems that do not include Gpedit.msc and for an optional resolution, you can directly check and change the NoDriveTypeAutoRun entry value in the following registry key other than 0xFF.

   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Polic []() es\Explorer\`

   `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\`

Command prompt (Cmd. exe) command-line string limitation

Article • 09/23/2021 • 2 minutes to read

This article discusses the limitation to the length of the strings that you use from the command prompt in Command Prompt (Cmd.exe). It also provides methods that you can use to work around this limitation.

Applies to: Windows Server 2012 R2, Windows Server 2008 R2 Service Pack 1, Windows 7 Service Pack 1
Original KB number: 830473

More information

The maximum length of the string that you can use at the command prompt is 8191 characters.

This limitation applies to:

- the command line
- individual environment variables that are inherited by other processes, such as the PATH variable
- all environment variable expansions

If you use Command Prompt to run batch files, this limitation also applies to batch file processing.

Examples

The following examples show how this limitation applies to commands that you run in Command Prompt, and commands that you use in a batch file.

- In Command Prompt, the total length of the following command line can't contain more than 8191 characters:

  ```
  Console

  cmd.exe /k ExecutableFile.exe parameter1, parameter2... parameterN
  ```

- In a batch file, the total length of the following command line can't contain more than 8191 characters:

```
Console

cmd.exe /k ExecutableFile.exe parameter1, parameter2... parameterN
```

This limitation applies to command lines that are contained in batch files when you use Command Prompt to run the batch file.

- In Command Prompt, the total length of `EnvironmentVariable1` after you expand `EnvironmentVariable2` and `EnvironmentVariable3` can't contain more than 8191 characters:

```
Console

c:> set EnvironmentVariable1 = EnvironmentVariable2
EnvironmentVariable3
```

- In a batch file, the total length of the following command line after you expand the parameters can't contain more than 8191 characters:

```
Console

ExecutableFile.exe parameter1 parameter2
```

- Even though the Win32 limitation for environment variables is 32,767 characters, Command Prompt ignores any environment variables that are inherited from the parent process and are longer than its own limitations of 8191 characters (as appropriate to the operating system). For more information about the `SetEnvironmentVariable` function, see SetEnvironmentVariableA function.

How to work around the limitation

To work around the limitation, use one or more of the following methods, as appropriate to your situation:

- Modify programs that require long command lines so that they use a file that contains the parameter information, and then include the name of the file in the command line.

  For example, instead of using the `ExecutableFile.exe Parameter1 Parameter2... ParameterN` command line in a batch file, modify the program to use a command line that is similar to the following command line, where *ParameterFile* is a file that contains the required parameters (parameter1 parameter2... ParameterN):

Console

```
ExecutableFile.exe c:\temp\ParameterFile.txt
```

- Modify programs that use large environment variables so that the environment variables contain less than 8191 characters.

  For example, if the PATH environment variable contains more than 8191 characters, use one or more of the following methods to reduce the number of characters:
  - Use shorter names for folders and files.
  - Reduce the depth of folder trees.
  - Store files in fewer folders so that fewer folders are required in the PATH environment variable.
  - Investigate possible methods that you can use to reduce the dependency of PATH for locating .dll files.

Upgrade and Privacy Experience (UPX) is displayed in the UI on managed Windows 10 device

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue in which UPX is displayed in the user interface (UI) on a managed Windows 10 device.

Applies to: Windows 10 - all editions
Original KB number: 4016551

> **Note**
>
> This article is intended for managed environment scenarios. These steps not only suppress the UPX but also enable the devices to be considered as "managed" for the Windows 10 Creators Update.

Symptoms

Assume that you have a Windows 10-based computer that's configured to receive updates from the Microsoft Windows Update server. The computer is not domain-joined or Azure Active Directory Domain-joined or managed by a System Center Configuration Manager (SCCM) client, but the computer is otherwise managed, for example by an IT professional.

In this situation, the Upgrade and Privacy Experience (UPX) may be displayed in the user interface (UI) unexpectedly, contrary to the preferences of the IT professional or other person who manages the device.

Workaround

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a

problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

To work around this issue, follow these steps to suppress the UPX display and migrate existing privacy settings automatically instead of giving users of the device the opportunity to select privacy settings manually from the UPX UI:

1. Create the following registry key if it is not present on the system:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CreatorsUpdatePrivacySettings`

2. Create a new value named *ShowUI* of type REG_DWORD if it does not already exist, and set ShowUI to 0.

3. Create a new value named *AutoSet* of type REG_DWORD if it does not already exist, and set AutoSet to 0.

4. With the UPX UI suppressed, the existing privacy settings on the system will be migrated automatically when the Creators Update is applied. As part of your ongoing device management, we recommend you continue to review and manage privacy settings on the device, for example, by applying privacy-related group policies.

> **Note**
>
> Any client that is managed by third-party enterprise management software can also avoid the UPX UI display by having the two registry key values set.

For more information about UPX, see Choose your privacy settings for the Windows 10 Creators Update.

> **Note**
>
> If the **KB4013214** update is already installed on the system, open **Task Scheduler**, navigate to \Microsoft\Windows\UNP, and run the `RunCampaignManager` command. This operation will prevent the UPX UI from being shown to the end user even if the UPX has already been downloaded and installed on the system.

Status

Microsoft has confirmed that this is a problem in Windows 10 - all editions.

Unable to open high-resolution file in Windows Photo Gallery

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where users can't open high-resolution file in Windows Photo Gallery.

Applies to: Windows Vista
Original KB number: 2725211

Symptoms

Consider the following scenario:

- You start Windows Photo Gallery
- You select File, then choose Import From Camera or Scanner.
- You then import a high-resolution image. For example, you use a high-resolution scanner to scan a full-page document at a resolution of 1200 dpi. Alternately, you try to view a previously created image that is high resolution (such as a 1200-dpi full-page scan) using Windows Photo Gallery.

In this scenario, Windows Photo Gallery will fail to display the image, and will display the following message:

Photo Gallery can't open this picture or video. This file format is not supported, or you don't have the latest updates to Photo Gallery.

Cause

This problem occurs because, by default, Windows Photo Gallery will not open an image file that is larger than 100 megapixels.

For example, if you scan a full 8.5x11" page using a resolution of 1200 dpi, the resulting image file will be large (approximately 136 megapixels). This exceeds the default size limit for Windows Photo Gallery.

Resolution

To work around this issue:

When scanning an image, reduce the size of the image by scanning a smaller area (not a full page), or by using a lower resolution, such as 600 dpi or less. This will allow Windows Photo Gallery to open the scanned image successfully.

Alternately, you can override Windows Photo Gallery's image size limit by editing the registry:

1. Click Start, type regedit in the Start Search box, and then click regedit.exe in the Programs list. If you are prompted for an administrator password or for confirmation, type a valid password, or click Continue.
2. Locate and then click the following subkey in the registry:
   `HKEY_CURRENT_USER\Software\Microsoft\Windows Photo Gallery\Viewer`
3. Click Edit, click New, and then click DWORD (32-bit) Value.
4. Type MaximumFrameSizeMegapixels for the value name, and then press ENTER.
5. Double-click the MaximumFrameSizeMegapixels value, click Decimal, enter a new value in the Value data box, and then click OK.
6. Exit Registry Editor.
7. Restart Windows Photo Gallery. The Value data to enter is the maximum image size that Windows Photo Gallery will be able to open, in megapixels. For example, entering a value of 150 will allow Windows Photo Gallery to open files of up to 150 megapixels in size. This value would be sufficient to allow viewing of 1200 dpi full-page scans.

> ⓘ **Note**
>
> Entering a value of 0 will disable the image size limit. However, this is not recommended, because if Windows Photo Gallery then attempts to open a large or corrupt file, it could potentially result in a hang or crash.

Display configuration reverts to "Second screen only" after you resume from standby

Article • 12/06/2021 • 2 minutes to read

This article provides a workaround to an issue in which display configuration reverts to "Second screen only" after you resume from standby.

Applies to: Windows 10 - all editions
Original KB number: 2890797

Symptoms

On a Windows 10 or Windows 8-based laptop computer, you do the following:

1. Plug in an external monitor.
2. Change the display configuration to **Second screen only** (using the Windows logo key +P keyboard shortcut).
3. Change the display configuration to **Duplicate** (using the Windows logo key +P keyboard shortcut again).
4. Close the lid on the laptop computer.
5. Unplug the external monitor.
6. Open the lid on the computer.
7. Plug the external monitor back in.

In this scenario, the display configuration may revert to **Second Screen only** instead of remaining in **Duplicate** mode.

Cause

Microsoft has confirmed that this is a problem in the Microsoft products that are listed in the "Applies to" section.

Workaround

To work around this problem, use the Windows logo key) +P keyboard shortcut to change the display configuration back to **Duplicate** mode.

When using USB-attached monitor, display configuration may not be retained after reboot

Article • 09/23/2021 • 2 minutes to read

This article explains an issue where the display configuration is retained after reboot when you use USB-attached monitor.

Applies to: Windows 10 - all editions
Original KB number: 2465368

Symptoms

On a computer running Windows 10, you attach a secondary monitor via a USB connection. For example, you may attach a USB Port Replicator device, containing a DVI or VGA port, to the USB port of a laptop computer.

After attaching the secondary monitor, the display configuration may default to "Extend" or "Duplicate." You may then change to a "Computer Only" configuration, in order to turn off the secondary monitor and use only the primary monitor. (You can select a different display configuration by pressing Windows + P keys on the keyboard.)

If you select a "Computer Only" configuration, and then reboot your computer, you may find that after rebooting, the configuration is changed back to "Extend," "Duplicate," or "Projector Only."

Cause

This behavior occurs because the driver for the USB video adapter enumerates the attached monitor after Windows has already initialized the video subsystem. Therefore, Windows believes the external monitor was plugged in after the computer had already finished booting. When a new monitor is plugged into a running system, Windows 7 attempts to switch to a configuration in which the new monitor is enabled.

Resolution

This is a known issue when using USB-attached displays in Windows.

More information

Windows 7 does not provide native support for video displays that are connected via USB. However, there are some proprietary systems available that enable this type of connection.

Display changes resolution in Windows 7 while pressing Win+P hot key and select duplicate when only one monitor is connected

Article • 09/23/2021 • 2 minutes to read

This article helps fix an issue where the display resolution may change to a lower resolution when you use the Presentation Display Mode keyboard shortcut (Windows logo key + P) to change the mode to Duplicate.

Applies to: Windows 7 Service Pack 1
Original KB number: 2518084

Symptoms

You will notice that the display resolution may change to a lower resolution when you use the Presentation Display Mode keyboard shortcut (Windows logo key + P) to change the mode to Duplicate in a Windows 7 Computer with only one monitor connected. This issue typically occurs on different models and brands of video graphic adapters when connected via DVI or Display Port.

Cause

This is expected behavior with video adapters that have multiple DVI or Display Port connections. Even though you only have one monitor physically connected to the video adapter, there are still other DVI/Display Port connections that are not used but available. When you change the Presentation Display Mode to Duplicate, the system will try to synchronize with the video port connections and will default to a compatible video resolution of a non-DVI/Display Port connection.

Resolution

To revert display resolution settings back to the previous setting. Use the Presentation Display Mode keyboard shortcut (Windows logo key +P) and change the mode to Computer only.

References

Windows 7 Keyboard shortcuts

Docking station external monitors not working when a Windows 10 version 1703-based portable computer is connected

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where an external monitor connected to a docking station doesn't work when a Windows 10 version 1703-based portable computer is connected.

Applies to: Windows 10
Original KB number: 4051625

Symptoms

Consider the following scenario:

- You have external monitors that are connected to a docking station.
- You have a portable computer that is running Windows 10 version 1703.
- In **Power Options**, the **Lid close action** setting is configured to "Do nothing."
- You turn on the computer and then close the lid.
- You attach the computer to the docking station.

In this scenario, the computer doesn't detect the external monitors. Therefore, the external monitors display a black screen.

Workaround

Use either of the following methods to force detection of the external monitors:

- Use the keyboard shortcut Win+Ctrl+Shift+B.
- In **Display Settings**, click the **Detect** button.

To work around this issue, use one of the following methods:

- Change **Lid close action** to any setting other than "Do nothing.". Before you make this change, make sure that the change does not affect your docking experience.
- Upgrade to Windows 10 Version 1709 that does not have this issue.

Error generated when Desktop Duplication API-capable application is run against discrete GPU

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an error that occurs when a Desktop Duplication API-capable application is run against a discrete GPU.

Applies to: Windows 8.1
Original KB number: 3019314

Symptoms

Consider the following scenario:

- You have a computer that is running Windows 8.1.
- You have a Desktop Duplication API (DDA)-capable application, and it calls the DDA to duplicate the desktop image.
- The display adapter on the computer is running under the Microsoft Hybrid system.

In this scenario, when the application tries to duplicate the desktop image against the discrete GPU on a Microsoft Hybrid system, the application may not run correctly, or it may generate one of the following errors:

> Failed to create windows swapchain with 0x80070005
>
> CDesktopCaptureDWM: IDXGIOutput1::DuplicateOutput failed: 0x887a0004

Cause

This issue occurs because the DDA does not support being run against the discrete GPU on a Microsoft Hybrid system. By design, the call fails together with error code DXGI_ERROR_UNSUPPORTED in such a scenario.

Resolution

To work around this issue, run the application on the integrated GPU instead of on the discrete GPU on a Microsoft Hybrid system.

More information

When this issue occurs, the IDXGIOutput1::DuplicateOutput method fails and returns an error code DXGI_ERROR_UNSUPPORTED.

For example, this DXGI desktop duplication sample is affected by this issue.

Some fonts may be scaled too large or too small when you change the DPI setting in Windows 7

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue that the fonts may not all get scaled properly when you change the DPI setting in Windows 7 Service Pack 1.

Applies to: Windows 7 Service Pack 1
Original KB number: 2556182

Symptoms

Consider the following scenario on a Windows 7 Service Pack 1 machine:

- Right-click on the desktop and click **Personalize**.
- Click **Display** to bring up the DPI adjustment window, which is titled **Make it easier to read what's on your screen**.
- Change from the current setting to a larger or smaller setting, then click **Log off now**.

When you perform these steps, sometimes the fonts may not all get scaled properly. Certain fonts in the user interface may be either too large or too small.

Cause

This is the result of a timing issue between the Explorer and Winlogon processes. When this condition happens, certain fonts get resized twice.

Resolution

Change the DPI setting again to reset the font to a normal size.

> ⓘ **Note**
>
> You may need to change the setting a few times.

Windows 8: List All Modes in Advanced Display Settings in Control Panel displays incomplete list of modes when in Duplicate mode

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where the list of available modes is different than the list displayed in Windows 7 when you use multiple displays in "Duplicate" mode in Windows 8.

Applies to: Windows 8
Original KB number: 2813712

Symptoms

Consider the following scenario:

The operating system is Windows 8 and you are using multiple displays in "Duplicate" mode. When selecting **Advanced Settings** in the Screen Resolution Control Panel and then selecting the **List All Modes** button on the **Adapter** tab of the monitor and display driver dialog box, the list of available modes is different than the list that is displayed in Windows 7.

Cause

This behavior is by design. The list of display modes available when "Duplicate" mode is selected on a Windows 8 client is based upon the selected primary monitor at the time of selecting Duplicate mode. In Windows 7, all display modes are displayed regardless of the primary monitor selection.

Resolution

If the desired display mode is not available in "Duplicate" mode, select a different monitor as the primary monitor prior to selecting "Duplicate" display mode.

Mouse input in some games is incorrectly scaled on high-DPI devices

Article • 09/23/2021 • 2 minutes to read

This article describes how to work around an issue in which mouse input in some games is incorrectly scaled on high-DPI devices.

Applies to: Windows 8.1
Original KB number: 2907016

Introduction

Windows 8.1 supports bitmap scaling of desktop application content for applications that don't natively support high-DPI displays. It also scales mouse, pen, and touch input that is sent to those applications. Scaling both input and output guarantees a consistent experience for the application user.

However, there are two scenarios in which scaling can be mismatched:

- Games that run in full-screen mode and bypass the output scaling of Windows (only input is scaled)
- Games that use "raw mouse input" in windowed mode and bypass the input scaling of Windows (only output is scaled)

Most Windows desktop applications don't use full-screen mode or raw input. However, games frequently use one or both configurations. Windows detects many full-screen games and exempts them from both input and output high-DPI scaling on successive starts. But this detection fails in some games and upgrade scenarios. In these cases, you may experience mouse input that is either consistently larger or consistently smaller than what is reflected on the screen. The effect can be seen either in the position of the pointer or the location at which you can interact with on-screen content.

Workaround

We recommend that you manually configure games to be exempt from output and input high-DPI scaling. This should be done only for specific applications. This is because a change in the global desktop DPI scaling settings affects other desktop applications and may cause content to be displayed too small to be usable.

To make these configurations, locate the game's executable binary, and then change the compatibility properties of that file. To do this, follow these steps:

1. Locate the game's executable binary. You can usually search for the file by using Windows 8.1 search, as follows:
   a. On the **Start** screen, type the name of the game application.
   b. Right-click or press and hold the application's icon, and then select **Open file location**.A folder that contains the start menu shortcut for the application will open.
2. Change the compatibility properties, as follows:
   a. Right-click or press and hold the file explorer icon for the application, and then select **Properties**.
   b. On the **Compatibility** tab, select the **Disable display scaling on high DPI settings** check box.
   c. Tap or click **Apply**, and then tap or click **OK**.

Additional troubleshooting tips

- For some games, the shortcut starts a "launcher" application that then starts the game. You may have to locate the actual game application and then apply this compatibility change to it.
- Some applications provide compatibility options within the application instead of using the application's **Properties** window. If this window doesn't have a **Compatibility** tab, determine whether the options within the application include the ability to disable high-DPI scaling.

Windows 10 Technical Preview adds a feature that blocks untrusted fonts

Article • 09/23/2021 • 5 minutes to read

This article describes a new feature that blocks untrusted fonts for Windows 10 Technical Preview. Before you use the feature, you can see the feature introduction and the potential reductions in functionality section. Then, follow the steps to configure the feature.

Applies to: Windows 10 - all editions
Original KB number: 3053676

The blocking untrusted fonts feature

Because fonts use complex data structures and can be embedded into webpages and documents, they can be vulnerable to elevation of privilege (EOP) attacks. EOP attacks mean that a malicious hacker can remotely access a user's computer when users share files or surf the web. To strengthen security against these attacks, we have created a feature to block untrusted fonts. Using this feature, you can turn on a global setting that stops users from loading untrusted fonts that are processed by the Graphics Device Interface (GDI). Untrusted fonts are any fonts that are installed outside the `%windir%/Fonts` directory. The blocking untrusted fonts feature helps stop both remote (web-based or email-based) and local EOP attacks that can occur during the font file-parsing process.

How does this feature work

There are three ways to use this feature:

- On. Helps stop any font being loaded that is processed by using GDI and is installed outside the `%windir/Fonts%` directory. It also turns on event logging.
- Audit. Turns on event logging, but does not block fonts from loading, regardless of location. The names of the applications that use untrusted fonts appear in your event log.

> **Note**

> If you are not ready to deploy this feature in your organization, you can run it in Audit mode to see if not loading untrusted fonts causes any usability or compatibility issues.

- Exclude apps to load untrusted fonts. You can exclude specific applications. It allows them to load untrusted fonts, even when the feature is turned on.

Potential reductions in functionality

After you turn on this feature, users might experience reduced functionality in following situations:

- Sending a print job to a shared printer server that uses this feature and where the spooler process has not been excluded. In this situation, any fonts that are not already available in the server's `%windir%/Fonts` folder will not be used.
- Printing using fonts provided by the installed printer's graphics .dll file, outside the `%windir%/Fonts` folder. For more information, see Introduction to Printer Graphics DLLs.
- Using first or third-party apps that use memory-based fonts.
- Using Internet Explorer to view websites that use embedded fonts. In this situation, the feature blocks the embedded font, causing the website to use a default font. However, not all fonts have all the characters, so the website might render differently.
- Using desktop Office to view documents that have embedded fonts. In this situation, content is displayed by using a default font picked by Office.

How to turn on and use the feature

To turn this feature on, off, or to use audit mode, use one of the following methods.

Use Group Policy

1. Open Local Group Policy Editor.
2. Under **Local Computer Policy**, expand **Computer Configuration**, expand **Administrative Templates**, expand **System**, and then click **Mitigation Options**.
3. In the **Untrusted Font Blocking** setting, you can see the following options:

    - **Block untrusted fonts and log events**

- **Do not block untrusted fonts**
- **Log events without blocking untrusted fonts**

Use Registry Editor

1. Open Registry Editor (regedit.exe) and go to the following registry subkey:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Kernel\
   ```

2. If the **MitigationOptions** key is not there, right-click and add a new **QWORD (64-bit) Value**, naming it as **MitigationOptions**.

3. Update the **Value data** of the **MitigationOptions** key, and make sure that you keep your existing value, like the important note below:

   - To turn on this feature, type 1000000000000.
   - To turn off this feature, type 2000000000000.
   - To audit with this feature, type 3000000000000.

   > **ⓘ Important**
   >
   > Your existing **MitigationOptions** values should be saved during your update. For example, if the current value is 1000, your updated value should be 1000000001000.

4. Restart your computer.

View the event log

After you turn on this feature, or start using Audit mode, you can check your event logs for detailed information.

Check the event log

1. Open the Event Viewer (eventvwr.exe) and go to the following path:

   Application and Service Logs/Microsoft/Windows/Win32k/Operational

2. Scroll down to EventID: 260 and review the relevant events.

   - Event example 1 - Microsoft Word

> ⓘ **Note**
>
> Because the FontType is Memory, there is no associated FontPath.

- Event example 2 - Winlogon

> ⓘ **Note**
>
> Because the FontType is File, there is also an associated FontPath.

- Event example 3 - Internet Explorer running in Audit mode

> ⓘ **Note**
>
> In Audit mode, the problem is recorded, but the font is not blocked.

Fix apps that have problems because of blocked fonts

Users may still need apps that have problems because of blocked fonts, so we suggest that you first run this feature in Audit mode to determine which fonts are causing the problems. After you figure out the problematic fonts, you can try to fix your apps in one of two ways: by directly installing the fonts into the %windir%/Fonts directory or by excluding the underlying processes and letting the fonts load. As the default solution, we highly recommend that you install the problematic font. Installing fonts is safer than excluding apps because excluded apps can load any font, trusted or untrusted.

Fix apps by installing the problematic fonts (recommended)

On each computer that has the app installed, right-click the font name, and then click **Install**.

The font should automatically install into your `%windir%/Fonts` directory. If it does not, you have to manually copy the font files into the Fonts directory and run the installation from there.

Fix apps by excluding processes

1. On each computer that has the app installed, open Registry Editor and go to the following registry subkey:

   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\<Process_Image_Name>`

   For example, if you want to exclude Microsoft Word processes, you would use `HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Winword.exe`.

2. If the **MitigationOptions** key is not there, right-click and add a new **QWORD (64-bit) Value**, naming it as **MitigationOptions**.

3. Add the value for the setting desired for that process:

   - To turn on this feature, type 1000000000000.
   - To turn off this feature, type 2000000000000.
   - To audit with this feature, type 3000000000000.

   > **Important**
   >
   > Your existing **MitigationOptions** values should be saved during your update. For example, if the current value is 1000, your updated value should be 1000000001000.

4. Add any additional processes that need to be excluded, and then turn font blocking on by using the steps that are provided in the Fix apps by excluding processes section.

Video resolution limits for H.264 and Video Stabilization in Windows 8 and Windows RT

Article • 09/23/2021 • 2 minutes to read

This article describes video resolution limits for H.264 and video stabilization.

Applies to: Windows 8
Original KB number: 2829223

Summary

H.264 support in Windows 8 and Windows RT is limited to 2048x2048 pixels for Encoding and Decoding. Sample Frames used by the Video Stabilization DSP are limited to 16k pixels by DirectX 2D.

More information

Encoder/Decoder

The H.264 standard only recognizes resolutions up to 2048x2048. The Microsoft H.264 (MP4) decoder/encoder is designed to only support video content up to the H.264 standard. The Microsoft H.264 (MP4) encoder/decoder supports any custom or standard resolution up to the 2048x2048 limit. The Microsoft H.264 (MP4) encoder/decoder supports any custom or standard aspect ratio.

Commonly supported resolutions and aspect ratios include:

- 854 x 480 (16:9 480p)
- 1280 x 720 (16:9 720p)
- 1920 x 1080 (16:9 1080p)
- 640 x 480 (4:3 480p)
- 1280 x 1024 (5:4)
- 1920 x 1440 (4:3)

Video Stabilization DSP

The Video Stabilization Digital Signal Processor (DSP) used by Windows 8 and Windows RT is based on a DirectX 2D implementation. DirectX 2D defines a 16k limit for the width of a buffer. The Video Stabilization DSP makes a DirectX 2D buffer that represents multiple frames; the contents of each row is a sample frame, and each row is the history of sample frames. Each row (sample frame) contains the pixels of 1/16th of a source frame (Width/16 x Height/16). Due to DirectX 2D's 16k limit per row, the effective maximum standard resolution supported for 16:9 and 4:3 are:

- 16:9 - 2560 x 1440 (Source Frame) = 160 x 90 (Sample Frame) = 14,400 pixels per row
- 4:3 - 2304 × 1728 (Source Frame) = 144 x 108 (Sample Frame) = 15,552 pixels per rowNote these Source Frame resolutions are both greater than the H.264 2048x2048 limit. Video Stabilization at these higher resolutions can be successfully utilized when not associated with H.264 encoding.

Camera application

In video mode, the Microsoft Store Camera application will report the error "Something went wrong while recording this video" when the camera's resolution is above the H.624 or Video Stabilization limits - at the time of capture, not at preview. To resolve this error, use a lower resolution or change the aspect ratio.

If the Camera application error is observed, contact the vendor of the camera - unsupported video resolutions should not be listed by the camera's driver. The camera driver can list resolutions higher than the video limit for image capture.

Can't set time zone automatically in Windows 10

Article • 03/04/2022 • 2 minutes to read

Applies to: Windows 10

> **Note**
>
> If you're not a support agent or IT professional, you'll find more helpful information in **How to set your time and time zone**.

Non-administrator users cannot change or interact with the **Set time zone automatically** setting. The setting is either not visible or is "greyed out" in the **Settings** app. This is by design as the **Set time zone automatically** setting is a system wide setting that applies to all user profiles on a machine.

To resolve this issue, the IT administrators should make sure the setting **Set time zone automatically** is enabled before deployment of a device. If the device is already deployed, you can use one of the following methods mentioned below to enable the setting.

Use Registry Editor

Run **Registry Editor** as an administrator and follow these steps:

1. Change the **Set time zone automatically** setting and set the data value of the registry entry `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\tzautoupdate\Start` as follows:

Value data	Result
3	Enable Set time zone automatically
4	Disable Set time zone automatically

2. Change the location setting and set the value of the registry entry `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager\ConsentStore\location\Value` as follows:

Value string	Result
Allow	On
Deny	Off

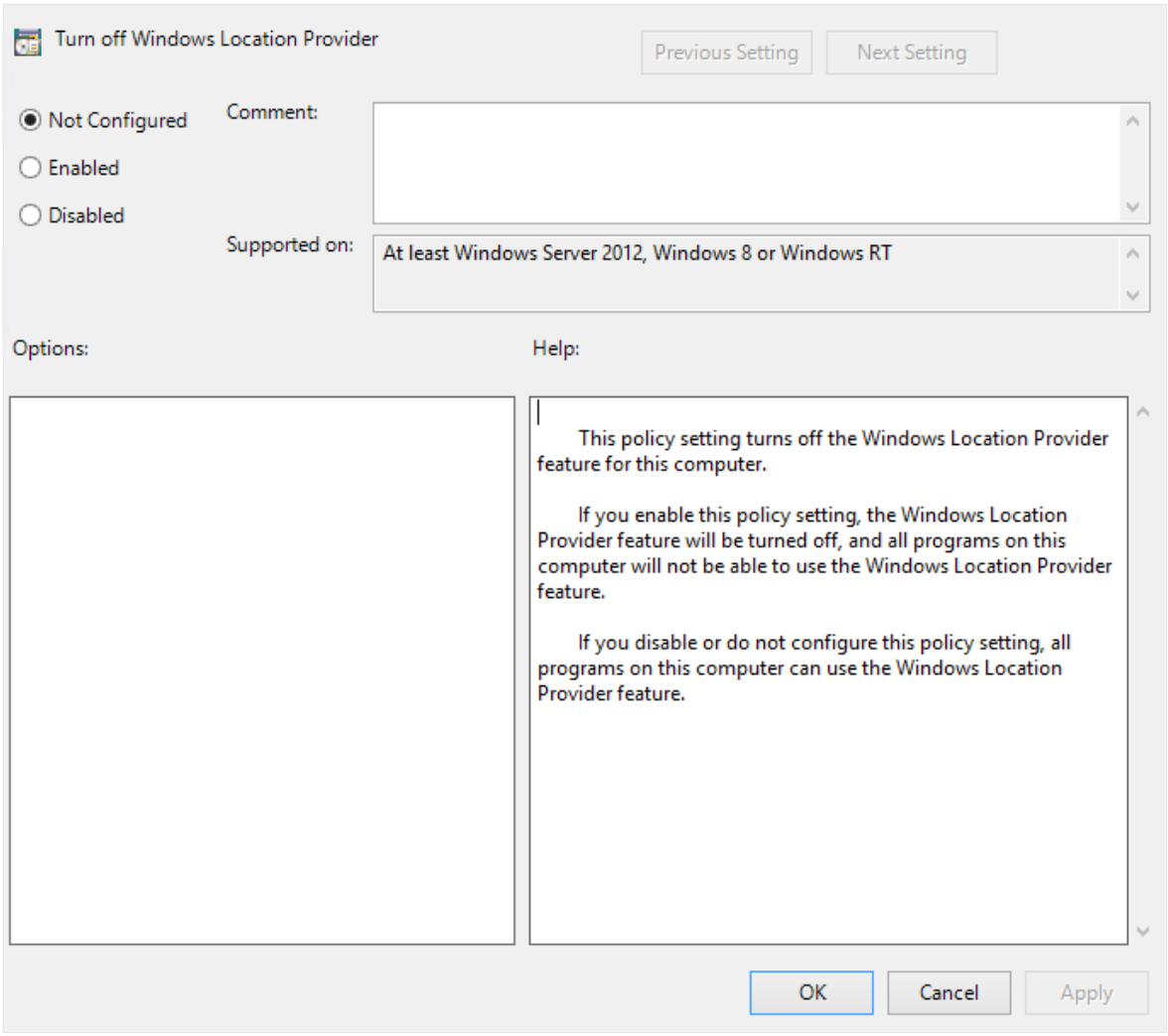
> **Note**
>
> If the **Location** setting is turned off by a group policy, you must reverse the policy otherwise it will override the manual editing of the entry.

Use Group Policy

To change the registry settings, use Group Policy Preferences to enable the **Set the time zone automatically** setting. Next, follow these steps to enable the **Location** setting in **Local Group Policy Editor**.

1. Go to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Location and Sensors** > **Windows Location Provider** > **Turn off Windows Location Provider**.

2. Set the value of the **Turn off Windows Location Provider** setting to **Not Configured** as follows:



Use MDM policy

Run a PowerShell script to change the registry settings in Microsoft Intune. Next, use the mobile device management (MDM) policy Privacy/LetAppsAccessLocation to enable the **Location** setting as follows:

Value	Result
0	User in control
1	Force allow
2	Force deny

> ⓘ **Note**
>
> The recommended value is *0*, but setting the value to *1* ensures that automatic time zone gets the correct location.

For more information about other options to control applications access to the location, see Privacy/LetAppsAccessLocation_ForceAllowTheseApps, Privacy/LetAppsAccessLocation_ForceDenyTheseApps and Privacy/LetAppsAccessLocation_UserInControlOfTheseApps.

Changes to calendar date in BIOS are not reflected in Windows

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution to an issue where changes to calendar date in BIOS are not reflected in Windows.

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 2792897

Symptoms

Consider the following scenario:

- You have a computer that runs Windows 8 or a later version, or Windows Server 2012 or a later version.
- In the computer BIOS, you change the calendar date to a value that is earlier than the date that Windows shows.
- You save the change, and you restart Windows

In this scenario, the Windows date setting does not reflect the change that you made to the calendar date in the BIOS.

Cause

This behavior is by design. Windows considers the fact that time does not travel backward. Also, the BIOS on a laptop or notebook device may report a date that is earlier than the Windows date if the battery is failing or dead. In such cases, the BIOS date and time are not reliable.

Resolution

If you have to change the calendar date on your computer, use the Windows settings to make the change instead of changing the date in the BIOS. This change will be reflected across multiple restarts.

More information

This behavior is new to Windows 8 and Windows Server 2012. Additionally, this behavior does not affect changes to the calendar date in the BIOS if the new date is later than the date that Windows reports.

Daylight saving time help and support

Article • 01/21/2023 • 3 minutes to read

This article describes the Microsoft policy in response to daylight saving time (DST) and time zone (TZ) changes.

Original KB number: 22803

Microsoft support policy in DST and TZ changes

Many applications and cloud services reference the underlying Windows operating system for DST and TZ information. To make sure that Windows has the latest and most accurate time data, Microsoft continuously monitors DST and TZ changes that are announced by governments around the world. Microsoft makes an effort to incorporate these changes to Windows and publishes updates through Windows Update (WU). Each DST and TZ update that's released through WU will have the latest time data and will also supersede any previously issued DST and TZ updates.

Refer to the following table for Microsoft support policy in DST and TZ changes:

Change type	Change details	Microsoft support policy	Solution

Change type	Change details	Microsoft support policy	Solution
Changes to a region's time zone rules	A subset of the region that shares a time zone makes a change to its DST requirements or changes the time bias of its time zone. A new time zone is required for the affected users within that region because the existing time zone has to remain unchanged for the rest of the users. -or- New DST or TZ change that doesn't match the exact parameters of another TZ, including historical time data accuracy (from 2010).	Microsoft will introduce a new time zone for such scenarios. A new Windows time zone entry will be created only when a country or region (including dependencies), or a first-order administrative division of a country or region (state, province, department, and so on), has a separate and distinct history of UTC offsets and DST rules from existing TZ entries. Additionally, a smaller geographic area (county, city, and so on) qualifies for a new Windows time zone entry when its current UTC offset and DST rule combination isn't provided by another Windows time zone entry. If there's insufficient lead time to engineer, test, and publish a Windows Update before these changes take effect, Microsoft will publish interim guidance on the DST Blog that can be used up until a Windows Update is made available.	Interim guidance and Windows Update
Changes to DST start and end dates	Modify an existing time zone by changing the DST rule or adding and removing DST to a time zone. -or- Modifying the time bias to an existing time zone.	Microsoft will publish a Windows Update that incorporates these DST changes to existing Windows time zones. To make sure that these updates are made available before these laws take effect, we recommend that governments provide ample notice (one year or more) prior to the change taking effect. If there's insufficient lead time to engineer, test, and publish a Windows Update before these changes take effect, Microsoft will publish interim guidance on the DST Blog that can be used up until a Windows Update is made available.	Interim guidance and Windows Update

Change type	Change details	Microsoft support policy	Solution
Changes to display names	A region that has an existing Windows time zone announces changes to the name referenced in the Windows time zone display name.	Microsoft will update the display name for the existing time zones for all supported languages and publish an update. If there's insufficient lead time to engineer, test, and publish a Windows Update before these changes take effect, Microsoft recommends using the existing time zone until a Windows Update is made available.	Windows Update

Microsoft recommendations

In order for Microsoft to provide an update at the earliest and ensure a seamless transition to the new DST and TZ policies, Microsoft recommends that governments provide the following:

- Ample advance notice (one year or more) of the planned change
- Official published confirmation of planned changes to DST or time zones
- Concentrated efforts to promote the change to affected citizens

Standalone DST updates

KB 914387 provides a list of DST updates that have been released. It also includes a short summary of the content that's included in each update. This allows a consistent means for customers and partners to be informed whenever such an update is made available.

Monthly rollups

DST updates are also included in monthly rollup releases. You can find more information about our monthly rollup releases here:

Windows 11 update history
Windows 10 and Windows Server 2016 update history
Windows 8.1 and Windows Server 2012 R2 update history
Windows 7 SP1 and Windows Server 2008 R2 SP1 update history
Windows Server 2022 update history
Windows Server 2012 update history
Windows Server 2008 SP2 update history

> **Note**
>
> Subscribe to the **Microsoft Daylight Saving Time & Time Zone Blog** to receive the latest updates on changes around the world.

Sometimes you cannot associate a program with an extension in Windows 7

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where you're unable to associate a file extension to an application in Windows 7.

Applies to: Windows 7 Service Pack 1
Original KB number: 2159999

Symptoms

You may not be able to associate a file extension to an application in Windows 7.

Cause

This may occur if the program you are attempting to associate with is not registered correctly.

Resolution

Follow the steps below:

1. Type *regedit* in the Run line or from an elevated CMD prompt.
2. Navigate to `Computer\HKEY_CLASSES_ROOT\Applications` and find your .exe name.
3. Navigate under its name to shell> open> command.
4. Under Default, make sure the application location points to the actual location of the executable.
5. Press OK and then try to reassociate the file type as you normally would.

Some .CHM files may not render properly on Windows Vista and Windows 7

Article • 09/23/2021 • 2 minutes to read

This article provides the steps for fixing the issue that some .CHM files do not render properly.

Applies to: Windows 7 Service Pack 1
Original KB number: 2021383

Symptoms

When attempting to open a Compiled HTML Help (.CHM) file on Windows Vista or Windows 7, the file may open but display one of the following messages instead of the expected content:

- > Navigation to the webpage was canceled.

- > Action canceled.

Cause

This will occur if the .CHM file has been flagged as downloaded from an untrusted source, such as the Internet.

Resolution

To resolve this issue, carry out the following steps:

1. Right-click the .CHM file and choose **Properties**.
2. On the **General** tab, click the button labeled **Unblock**.
3. Click **OK**.

More information

This behavior is a function of the Attachment Manager, which applies a Zone Identifier to files downloaded from any source that is considered untrusted or at risk, such as the Internet Zone.

Context menus are shortened when more than 15 files are selected

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where the Open, Print, and Edit items are missing from the context menu when you select multiple items in Windows Explorer.

Applies to: Windows 10 - all editions
Original KB number: 2022295

Symptoms

The following items may be missing from the context (right-click) menu when multiple items are selected in Windows Explorer.

- Open
- Print
- Edit

Cause

This is by design. These context menu items won't appear if selecting more than 15 items to avoid accidentally performing these actions on a large number of files.

Resolution

The following registry value may be modified to choose the number of files that may be selected while maintaining the context menu options.

- Path: HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer
- Name: MultipleInvokePromptMinimum
- Type: DWORD
- Default: 15 (decimal)

More information

The registry change will go into effect after logging off and back on, or after terminating Windows Explorer (Explorer.exe) and relaunching the process.

Note

A value of 16 is interpreted as unlimited for showing the options from the context menu, however it doesn't allow the actual opening of the documents selected if selecting more than 16. To allow the opening of more than 16 documents, set this key to a decimal value greater than the number of documents you wish to open. Microsoft recommends only increasing this value to a reasonable number in a controlled environment and only where users really need this value increased.

You may receive an error when burning files to disc

Article • 12/06/2021 • 2 minutes to read

This article provides a resolution to an error that occurs when burning files to disc.

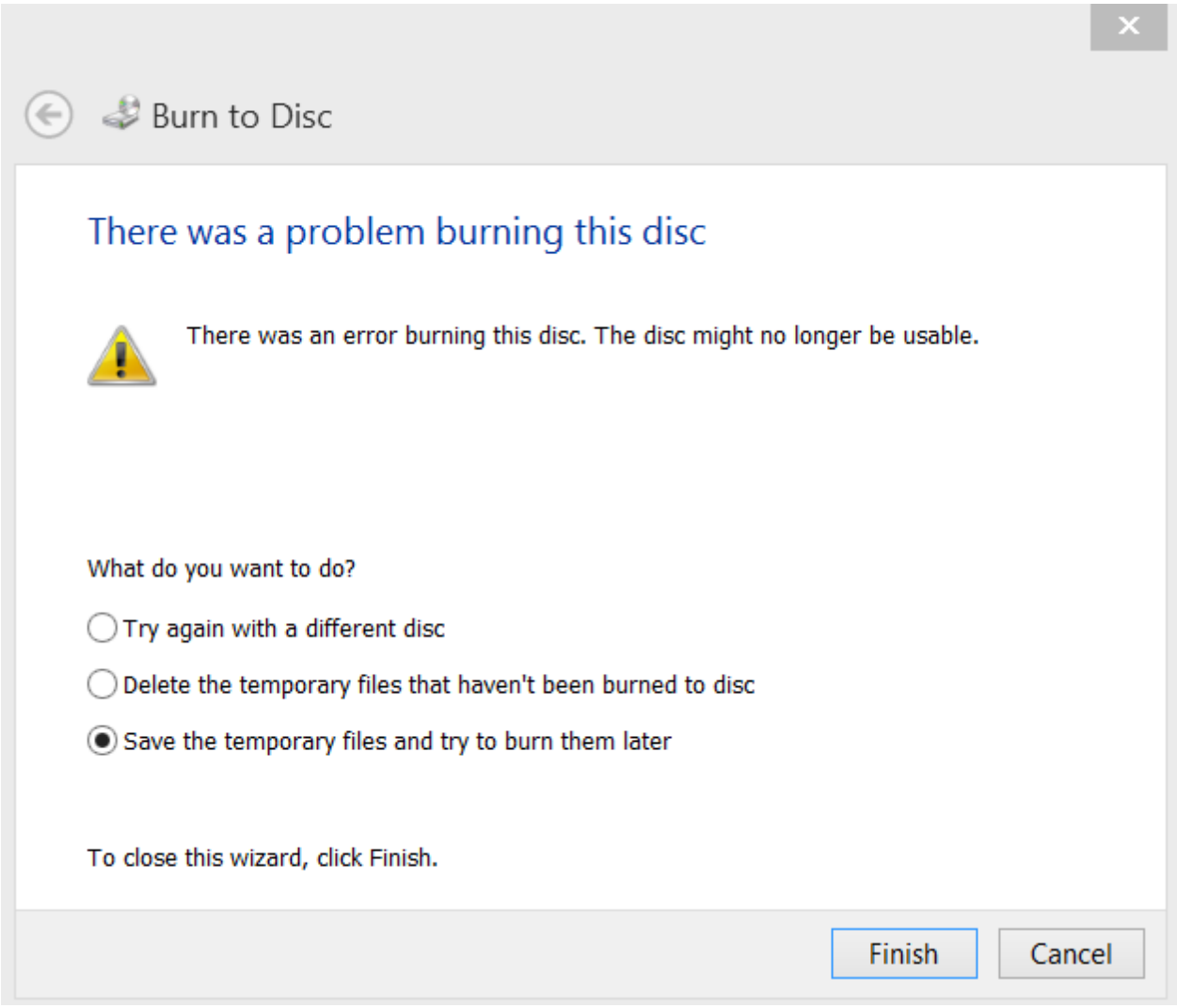
Applies to: Windows 8
Original KB number: 2748977

Symptoms

Consider the following scenario:

1. You have a Windows 8 computer with an optical disc drive that supports writing.
2. You insert a blank disc into the writer and select **Tap to choose what happens with blank DVDs**.
3. You select **Burn files to disc**.
4. The **Burn a Disc** window will appear.
5. You choose the **With a CD/DVD player** option.
6. You click the **Next** button to open up an **Explorer** window.
7. You drag a large file to the Explorer window that appeared in step 6.
8. While the copy is still active, you right click on the blank disc in the left hand pane of Explorer and select **Burn to disc** from the context menu.

After you do this, you receive the following error message:



Cause

This error occurs because the first copy session is still in progress. If you select **Burn to disc** again, Windows will attempt to burn files to the same drive again in a different session. This is not a supported scenario.

Resolution

Wait for the file copy to finish before starting **Burn to disc**.

Opening a Library in Windows Explorer gives error that it is no longer working

Article • 09/23/2021 • 2 minutes to read

This article provides a solution for fixing the error that shows it is no longer working when opening a Library in Windows Explorer.

Applies to: Windows 10 - all editions
Original KB number: 2895090

Symptoms

Consider the following scenario:

- You have a PC running Windows 7 or Windows 8.
- In Windows Explorer, you try to open a Library such as Documents, Music, Pictures or Videos.

In this scenario, when trying to open a library, you may encounter an error stating that it is no longer working. For example, accessing the Documents folder would cause the following error to appear:

> Documents.library-ms is no longer working.
> This library can be safely deleted from your computer. Folders that have been included will not be affected.

Cause

The link to the library has become corrupt.

Resolution

To resolve this issue, follow the steps below.

> **Note**
>
> Following these steps to delete and recreate the libraries will not affect any of the data in your libraries.

1. Open Windows Explorer.
2. On the left-hand pane, find **Libraries** and select it. If you do not see **Libraries** listed, click **View** on the menu at the top of the screen. Then click on the **Navigation pane** drop down and make sure that **Show libraries** has a check next to it.
3. Highlight all of the libraries (Documents, Pictures, Music, and Videos), right-click and choose **Delete**.
4. On the left-hand pane, select **Libraries**, right-click and choose **Restore default libraries**.

The libraries are then recreated and all of your data in the library folders should now be accessible again through the Windows Explorer Libraries.

How to remove the Security tab by using a group policy

Article • 09/23/2021 • 2 minutes to read

This article describes how an administrator can disable the **Security** tab from Windows 2000 Professional-based workstations that are members of a Windows 2000 domain.

Applies to: Windows 2000
Original KB number: 303153

Summary

Administrators can adjust registry permissions by using the security settings in a group policy. These settings are then applied to Windows 2000 Professional-based workstations during startup.

Remember that the assignment of registry permissions by using a group policy has similar results as using system policies because the results are permanent. To reverse these settings, you need to reverse the same policy and apply the new settings to the computer. Deleting the policy without reversing the settings results in the settings staying on the computer until a policy is created to reverse them or they are manually changed by using the Registry Editor tool.

Disable the Security tab

To disable the Security tab from Windows 2000 Professional-based workstations that are members of a Windows 2000 domain:

1. Start Active Directory Users and Computers.
2. Right-click the domain, and then click **Properties**.
3. Click the **Group Policy** tab on the domain properties dialog box to view the default domain policy.
4. Click **New**. **New Group Policy Object** should appear in the list of objects. Rename this Policy to Remove Security Tab. Make sure this policy is positioned directly under the default domain policy.
5. Click **Remove Security Tab**, and then click **Edit** to start the Group Policy Editor.

6. Expand **Computer Configuration** > **Windows Settings** > **Security Settings**, and then click **Registry**.
7. Right-click in the left pane, and then click **Add Key**.
8. Paste the following key in the text box, and then click **OK**:

   CLASSES_ROOT\CLSID\{1F2E5C40-9550-11CE-99D2-00AA006E086C}

   > ⓘ **Note**
   >
   > There may be a delay before you can proceed to the next step, and this is normal.

9. The **Database Security Editor** appears. You need to add the user or group that you want the **Security** tab to be removed from.
10. Change the permission on this key for the users and/or groups that you added in the previous step to "Deny Read." This prevents the user from being able to instantiate the needed components to display the Security and Sharing tabs. Click OK twice to complete the settings and exit the Group Policy Editor.

This policy will apply to computers upon the next policy refresh or when they're restarted. You can further control which computers will receive this policy by adding the computers to a group and use security filtering to either allow or deny this policy to be applied based on your environment.

How to use the Windiff.exe Utility

Article • 09/23/2021 • 4 minutes to read

This article describes how to use the Windiff.exe utility, a tool that graphically compares the contents of two ASCII files, or the contents of two folders that contain ASCII files, to verify whether they are the same. The file byte count and the creation date are not reliable indications.

Applies to: Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 159214

Summary

Sometimes you may experience unusual program behavior and may suspect that a file is damaged, or you may suspect that two files have the same byte count but different dates. Therefore, you want to make sure that they are the same. If a file is suspect, the typical solution is to recopy from a known good file. This solution may solve the problem, but it prevents you from knowing whether the original file was damaged. It can be important to determine this, as file damage can indicate an underlying network or system problem.

More Information

In Microsoft Windows 2000 and later, Windiff.exe is included on the original CD-ROM in the Support\Tools folder. To install the support tools, run Setup.exe from the Support\Tools folder. Windiff.exe is also in the Support.cab file. Support.cab is included with every service pack.

In Microsoft Windows NT, Windiff.exe is included in the Windows NT 4.0 Resource Kit. To download the Windows NT 4.0 Resource Kit Support Tools, visit the following Microsoft Web site:
MS Windows NT 4.0 Resource Kit Support Tools

The Windiff.exe utility graphically illustrates the differences between ASCII text files that you specify, or the difference between folders that contain ASCII text files, and is especially useful for comparing program source code. You can use Windiff.exe to compare whole subfolder trees. The display shows either a summary of the comparison status of a list of files (outline mode) or a detailed line-by-line comparison of the files (expanded mode).

To compare two files by using Windiff.exe, follow these steps:

1. Start Windiff.exe.
2. On the **File** menu, click **Compare Files**.
3. In the **Select First File** dialog box, locate and then click a file name for the first file in the comparison, and then click **Open**.
4. In the **Select Second File** dialog box, locate and then click a file name for the second file in the comparison, and then click **Open**.

   The information in the right pane indicates whether there is a file difference.
5. To view the actual file differences, click the first line in the Windiff.exe output results, and then on the **Expand** menu, click **Left File Only**, **Right File Only**, or **Both Files**.

   The color-coded results indicate what the file differences are.

To compare two folders by using Windiff.exe, follow these steps:

1. Start Windiff.exe.
2. On the **File** menu, click **Compare Directories**.
3. In the **Select Directories** dialog box, type the two folder names that you want to compare in the **Dir1** and **Dir2** boxes. If you want to include subfolders, click to select the **Include subdirectories** check box.

   The information in the right pane indicates the differences between the two folders.
4. To view the actual file differences, click the line that you want in the Windiff.exe output results, and then on the **Expand** menu, click **Left File Only**, **Right File Only**, or **Both Files**.

   The color-coded results indicate what the file differences are.

You can also run Windiff.exe from the command line. For information about how to do so, or for more information about how to use Windiff.exe, see the Windiff.exe Help file (Windiff.hlp).

There are other utilities that are available besides Windiff.exe that you can use to compare local ASCII and binary files, or to compare a local file to a questionable file at a remote site.

To compare two files or groups of files at a local site, you can use the Fc.exe and the Comp.exe file compare commands. Both commands are run from a command prompt.

You can use Fc.exe to compare two ASCII or binary files on a line-by-line basis. It offers several command-line options. For example, use the `fc /b` command to compare two binary files. For a complete list of options, type `fc /?` at a command prompt.

You can use Comp.exe to compare ASCII and binary files and to compare groups of files in two different folders. For example, to compare all the .dll files in one folder to all the .dll files in the same folder on a different computer, type the following at a command prompt:

Console

```
comp C:\Winnt\System32\*.dll \\DifferentComputerName\C$\Winnt\System32\*.dll
```

To compare a local file to a remote file, you can use a utility such as the third-party compression utility Pkzip.exe. To do so, use Pkzip.exe to zip the file at both the local and the remote sites. Because zipping a large file can take time, it is faster to use the pkzip -e0 (no compression) option. After you have zipped the files, use the `pkzip -v` command to examine the cyclic redundancy check (CRC32) value for the .zip files. If the CRC32 values are the same for the remote and local sites, the files are the same.

> **Note**
>
> If you use Pkzip.exe to zip a file before you send the file to a remote site, because of the embedded CRC32, you will receive an error message during the unzip process if the file is damaged in transit. If you receive no error message, the file was conveyed without damage.

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, regarding the performance or reliability of these products.

Renaming a network folder in Windows 7 Explorer fails with "the action can't be completed..."

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where Renaming a network folder in Windows 7 Explorer fails.

Applies to: Windows 7 Service Pack 1
Original KB number: 2025703

Symptoms

Steps to reproduce the issue:

1. Map a drive to a network share that contains several subfolders that contains images files or PDFs
2. Open an Explorer window and navigate to the parent folder.
3. Attempt to rename each folder successively, while drilling into the subfolder contents.
4. Continue step 3 until an error dialog containing the following text appears indicating that the subfolder cannot be renamed:
   "The action can't be completed because the folder or a file in it is open in another program. Close the file or folder and try again."

Cause

The folder rename operation fails because thumbcache.dll still has an open handle to the local thumbs.db file and does not currently implement a mechanism to release the handle to the file in a more dynamic and timely fashion.

Resolution

To work around the issue, enable User Group Policy setting for "Turn off the caching of thumbnails in hidden thumbs.db files":

Policy Path `User Configuration\Administrative Templates\Windows Components\Windows Explorer`
Policy Setting "Turn off the caching of thumbnails in hidden thumbs.db files"
Policy Value Enabled

> **Important**

This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:
322756 How to back up and restore the registry in Windows

You can directly edit the registry with the following setting:

Registry path `HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer`
Setting Name `"DisableThumbsDBOnNetworkFolders"`
Type REG_DWORD
Value 1

Another workaround is to wait approximately 1-5 minutes then retry the rename operation.

Support for Whitespace characters in File and Folder names for Windows

Article • 09/23/2021 • 3 minutes to read

This article describes support for whitespace characters in file and folder names.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2829981

Summary

File and Folder names that begin or end with the ASCII Space (0x20) will be saved without these characters. File and Folder names that end with the ASCII Period (0x2E) character will also be saved without this character. All other trailing or leading whitespace characters are retained.

For example:

- If a file is saved as ' Foo.txt', where the leading character(s) is an ASCII Space (0x20), it will be saved to the file system as 'Foo.txt'.
- If a file is saved as 'Foo.txt ', where the trailing character(s) is an ASCII Space (0x20), it will be saved to the file system as 'Foo.txt'.
- If a file is saved as '.Foo.txt', where the leading character(s) is an ASCII Period (0x2E), it will be saved to the file system as '.Foo.txt'.
- If a file is saved as 'Foo.txt.', where the trailing character(s) is an ASCII Period (0x2E), it will be saved to the file system as 'Foo.txt'.
- If a file is saved as ' Foo.txt', where the leading character(s) is an alternate whitespace character, such as the Ideographic Space (0x3000), it will be saved to the file system as ' Foo.txt '. The leading whitespace characters are not removed.
- If a file is saved as 'Foo.txt ', where the trailing character(s) is an alternate whitespace character, such as the Ideographic Space (0x3000), it will be saved to the file system as 'Foo.txt '. The trailing whitespace characters are *not* removed.File and Folder names that begin or end with a whitespace character are enumerated differently by the Win32 and WinRT APIs due to ecosystem requirements.

More information

Whitespace Characters

There are various whitespace characters representing various 'space' widths (glyphs). Only the ASCII Space (0x20) and ASCII Period (0x24) characters are handled specially by the Object Manager. Although the Ideographic Space character (0x3000) is also generated by using the Spacebar (when IME is enabled), it is not handled specially.

- 0x0020 SPACE
- 0x00A0 NO-BREAK SPACE
- 0x1680 OGHAM SPACE MARK
- 0x180E MONGOLIAN VOWEL SEPARATOR
- 0x2000 EN QUAD
- 0x2001 EM QUAD
- 0x2002 EN SPACE
- 0x2003 EM SPACE
- 0x2004 THREE-PER-EM SPACE
- 0x2005 FOUR-PER-EM SPACE
- 0x2006 SIX-PER-EM SPACE
- 0x2007 FIGURE SPACE
- 0x2008 PUNCTUATION SPACE
- 0x2009 THIN SPACE
- 0x200A HAIR SPACE
- 0x200B ZERO WIDTH SPACE
- 0x202F NARROW NO-BREAK SPACE
- 0x205F MEDIUM MATHEMATICAL SPACE
- 0x3000 IDEOGRAPHIC SPACE
- 0xFEFF ZERO WIDTH NO-BREAK SPACE

Object Manager

ASCII Space (0x20) characters at the beginning or end of a file or folder name are removed by the Object Manager upon creation.

ASCII Period (0x2E) characters at the end of a file or folder name are removed by the Object Manager upon creation.

All other leading or trailing whitespace characters are retained by the Object Manager.

API Enumeration

Win32 API

The Win32 API (CreateFile, FindFirstFile, etc.) uses a direct method to enumerate the files and folders on a local or remote file system. All files and folders are discoverable regardless of the inclusion or location of whitespace characters.

WinRT API

The WinRT API is designed to support multiple data providers (Physical Drives, OneDrive, Facebook, etc.). To achieve this, WinRT API uses a search engine to enumerate files and folders. Due to the search approach to enumeration, the WinRT API (StorageFile, StorageFolder, etc.) does not handle file and folder names with trailing whitespace characters other than ASCII Space (0x20) and ASCII Period (0x2E) residing on a local or remote file system. It does handle leading non-ASCII whitespace characters.

Observed Behavior

File Explorer and Desktop applications

All files and folders are visible within File Explorer and Desktop applications regardless of inclusion or location of whitespace characters.

Microsoft Store applications

When using the File Picker, files with a trailing non-ASCII whitespace character do not appear. The contents of subfolders with trailing non-ASCII whitespace characters are not displayed in the File Picker. Files or folders containing a leading non-ASCII whitespace character are displayed.

Lock screen isn't displayed when you resume a Windows 10-based computer

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue that prevents the lock screen from being displayed when you try to resume a Windows 10-based computer from Away Mode.

Applies to: Windows 10, version 1903, Windows 10, version 1809
Original KB number: 3205123

Symptoms

Consider the following scenario:

- You have a computer that has Intel® Ready Mode enabled.
- You install Windows 10 on the computer.
- You try to resume the computer from Away Mode. In this scenario, the Windows Lock screen isn't displayed as expected.

Workaround

The Windows Lock screen will be displayed when you press or select any human interface device (HID) such as a keyboard or mouse.

Status

Microsoft has confirmed that this is a problem in the Microsoft products that are listed at the beginning of this article.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

How to Manage the Lock Screen Image on Windows 8 and Windows Server 2012

Article • 09/23/2021 • 2 minutes to read

This article describes how an administrator can manage the lock screen image.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2787100

Symptoms

Scenario:

You have deployed Windows 8 and or Windows Server 2012 servers.

You want to use a customized lock screen image on these systems.

You want a centrally managed method of deploying the customized lock screen image.

Resolution

The update "Windows 8 and Windows Server 2012 cumulative update: November 2012" adds functionality to the Control Panel group policies that allow an administrator to designate a lock screen image on their Windows 8 and Windows 2012 computers. This setting lets you specify the default lock screen image shown when no user is signed in, and also sets the specified images as the default for all users (it replaces the inbox default image) Some restriction apply. See the Restrictions section below.

The new group policy is named "Force a specific default lock screen image" and can be found in this path in the group policy editor: "Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization"

Requirements:

To deploy the new "Force a specific default lock screen image" GP the following requirements must be met:

1. The update "Windows 8 and Windows Server 2012 cumulative update: November 2012" must be applied to all Windows 8 and Windows Server 2012 computers that you want to deploy customer lock screen images to. This is required as the Control Panel group policy client-side extension must be updated to enforce the group policy.

2. The group policy used to deploy the custom lock screen image must be edited on a machine that has been patched with "Windows 8 and Windows Server 2012 cumulative update: November 2012".

Restrictions

- Windows 8 Enterprise or Windows Server 2012 can use the new GP "Force a specific default lock screen image" via Domain GP or via local GP.
- Windows 8 Pro can also be a target of the GP if the machine is joined to a domain.

Implementation Steps for Domain Based Group Policy

1. Patch all system with update "Windows 8 and Windows Server 2012 cumulative update: November 2012" KB 2770917.

2. Create a GPO and link it to the OU where the computer accounts are located that you want to deploy the custom lock screen image to. Alternatively you can use an existing GPO.

    a. Open the Group Policy Management Console (GPMC).

    b. Create and link a GPO to an OU or Locate an existing GPO that you want to use.

3. Create and link a GPO to an OU or Locate an existing GPO that you want to use.

    a. In GPMC right-click the GPO from step 2b and select edit.

    b. Go this path "Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization".

    c. Enable the GP "Force a specific default lock screen image".

    d. Specify the path to the image file. It's recommended to use a DFS network path to provide redundancy.

4. After Sysvol replication has occurred and clients have refreshed their group policy settings the new lock screen will be used.

Implementation Steps for Local Group Policy

1. Patch the system with update "Windows 8 and Windows Server 2012 cumulative update: November 2012" KB 2770917.
2. Edit Local Policy.
    a. Run GPEDIT.MSC.
    b. Go this path "Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization".
    c. Enable the GP "Force a specific default lock screen image".
    d. Specify the path to the image file.
    e. Click OK.
3. Policy will be enforced as the next GP background refresh.

Monitor powers off after 1 minute when PC is locked

Article • 07/22/2022 • 2 minutes to read

This article describes a by-design behavior that computer monitor turns off after 1 minute when the computer is locked and provides a solution to solve this issue.

Applies to: Windows 8, Windows 8.1, Windows 10, Windows 11
Original KB number: 2835052

Symptoms

Consider the following scenario:

- You have a computer running Windows 8 or a later version of Windows.
- You lock the PC. For example, using the Windows Key+L keyboard shortcut or pressing Ctrl+Alt+Del and selecting "Lock".

In this scenario, you may observe that the PC monitor turns off after 1 minute. Changing the setting "Choose when to turn off the display" under Power Options in Control Panel does not change this behavior. This setting can be used to adjust the display timeout used when a user is logged in and idle but does not affect the timeout used when the PC is locked.

Cause

This behavior is by design in Windows. By default, when the console is locked, Windows waits for 60 seconds of inactivity before powering off the display. This setting is not configurable using the Windows user interface by default.

Resolution

Using the PowerCfg.exe utility, you can configure the display timeout used when the PC is in an unlocked state as well as when it is at a locked screen. From an administrative command prompt, the following commands can be used to control the display timeout:

- `powercfg.exe /setacvalueindex SCHEME_CURRENT SUB_VIDEO VIDEOIDLE \<time in seconds>`

- `powercfg.exe /setacvalueindex SCHEME_CURRENT SUB_VIDEO VIDEOCONLOCK \<time in seconds>`
- `powercfg.exe /setactive SCHEME_CURRENT`

The VIDEOIDLE timeout is used when the PC is unlocked and the VIDEOCONLOCK timeout is used when the PC is at a locked screen.

> ⓘ **Note**
>
> Using Powercfg commands to set the timeout only affects the current power scheme where the system is plugged in and using AC power. To set the timeouts used when on DC (battery) power, use the **/setdcvalueindex** switch instead of the **/setacvalueindex** switch.

Resolution for Windows 10 and Windows 11

In Windows 10 and Windows 11, you can expose the **Console Lock Display Off Timeout** setting under **Change Plan Settings**. From an administrative command prompt, the following commands can be used to expose the control.

Console

```
powercfg.exe -attributes SUB_VIDEO 8EC4B3A5-6868-48c2-BE75-4F3044BE88A7 -ATTRIB_HIDE
```

To hide the option, run the following command:

Console

```
powercfg.exe -attributes SUB_VIDEO 8EC4B3A5-6868-48c2-BE75-4F3044BE88A7 +ATTRIB_HIDE`
```

Microsoft Store doesn't open after a domain-joined computer makes a VPN connection

Article • 10/18/2021 • 2 minutes to read

This article discusses an issue in which you can't open Microsoft Store after a domain-joined computer connects to a VPN connection that has force tunneling enabled.

Applies to: Windows 10 – all editions
Original KB number: 4537233

Symptoms

Assume that you connect a domain-joined Windows 10 computer to a VPN connection that has force tunneling enabled. When you try to open Microsoft Store, it doesn't open, and you receive a "This page failed to load" error message.

If you do one of the following operations, Microsoft Store opens as expected:

- Disconnect the computer from the domain, and then connect to the VPN connection.
- Connect the computer to a VPN connection that has force tunneling disabled.
- Turn off the **Windows Defender Firewall** service, and then connect the computer to the VPN connection.

Cause

The Microsoft Store app uses a security model that depends on network isolation. Specific network capabilities and boundaries must be enabled for the store app, and network access must be allowed for the app.

When the Windows Firewall profile isn't **Public**, a default block rule blocks all outgoing traffic that has the remote IP set as **0.0.0.0**. While the computer is connected to a VPN connection that has force tunneling enabled, the default gateway IP is set as **0.0.0.0**. If the network access boundaries aren't set appropriately, the following behaviors occur:

- The default block firewall rule is applied.
- Microsoft Store app traffic is blocked.

Resolution

To fix this issue, follow these steps to create a Group Policy object (GPO):

1. Open the Group Policy Management snap-in (gpmc.msc), and create, or open a Group Policy for editing.
2. From the Group Policy Management Editor, expand **Computer Configuration** > **Policies** > **Administrative Templates** > **Network**, and then select **Network Isolation**.
3. In the right pane, double-click **Private network ranges for apps**.
4. In the **Private network ranges for apps** dialog box, select **Enabled**.
5. In the **Private subnets** text box, type the IP range of your VPN adapter, and then select **OK**.

   For example, If your VPN adapter IPs are in the 172.x.x.x range, add **172.0.0.0/8** in the text box.
6. Double-click **Subnet definitions are authoritative**, select **Enabled**, and then select **OK**.
7. Restart the client to make sure that the GPO takes effect.

After the Group Policy is applied, the added IP range is the only private network range that's available for network isolation. Windows will now create a firewall rule that allows the traffic, and will override the previous outbound block rule with the new rule.

> ⓘ **Note**
>
> - When your VPN address pool range changes, you should change this GPO accordingly. Otherwise, the issue will recur.
> - You can push the same GPOs from the DC to multiple computers.
> - On the individual computers, you can check the following registry location to make sure that the GPO takes effect:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkIsolation`

More information

You can use the "checknetisolation" built-in tool to check the network capabilities. When the computer is connected to the domain profile and VPN force tunneling, the InternetClient and InternetClientServer capabilities aren't active. For example:

Console

```
C:\Windows\system32>checknetisolation Debug -
n=microsoft.windowsstore_8wekyb3d8bbwe

Network Isolation Debug Session started.
Reproduce your scenario, then press Ctrl-C when done.
      Collecting Logs.....

Summary Report

Network Capabilities Status
----------------------------------------------------------------------
    InternetClient                Not Used and Insecure
    InternetClientServer          Not Used and Insecure
    PrivateNetworkClientServer    Missing, maybe intended


Network Capabilities Status
----------------------------------------------------------------------
    InternetClient                Used and Declared
    InternetClientServer          Not Used and Insecure
```

> **Note**
>
> On the same client, if you remove the computer from the domain or disconnect the VPN, you can see that **internetclient** is being used.

For more information, see Isolating Windows Store Apps on Your Network.

Error message in the Xbox Music app, Windows Media Player, Groove Music, or Movies &TV when you wake a Windows 10-based or Windows 8-based computer

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where playing audio whose source is a system that uses a DisplayPort or HDMI monitor fails.

Applies to: Windows 10, version 2004, Windows 10, version 1909, Windows 10, version 1809, Windows 10, version 1803, Windows 10, version 1709
Original KB number: 2841997

Symptoms

Consider the following scenario:

- You have a Windows 10-based or Windows 8-based computer that has a DisplayPort or HDMI monitor to which integrated audio is attached. Or, you have an all-in-one system that uses DisplayPort audio.
- You are playing audio by using the Xbox Music app, Windows Media Player, Groove Music, or Movies & TV, and the audio source is the monitor.
- While the audio is playing, you put the system to sleep. Then, you wake the system.

In this scenario, you may receive the following error message in the Xbox Music app on Windows 8:

Can't play. Make sure your computer's sound and video cards are working and have the latest drivers, then try again.

0xc00d11d1 (0xc00d4e86)

Or, you may receive the following error message in Windows Media Player on Windows 10 and Windows 8:

An audio device was disconnected or reconfigured. Verify that the audio device is connected, and then try to play the item again.

This issue also occurs when you use the Groove Music and Movies & TV app in Windows 10. When the issue occurs, you receive one or more of the following error messages:

Groove Music (audio file)

Can't play. We couldn't find your audio device are your headphones or speakers connected? If that's not it, you can go to the desktop and tap the speaker icon in the system tray for more help. 0xc00d4e86 (0xc00d4e86)

Movies & TV (video file)

Can't play. We couldn't find your audio device are your headphones or speakers connected? If that's not it, you can go to the desktop and tap the speaker icon in the system tray for more help. 0xc00d4e86 (0xc00d4e86)

Cause

This behavior is by design. When no other audio devices are connected to the system, the only audio endpoint on the system goes away when the monitor is powered off. Therefore, an error message is displayed by Xbox Music, Windows Media Player, Groove Music, or Movies & TV. The error messages will be displayed only on specific DisplayPort or HDMI monitors and will not occur if another audio output device is connected to the system.

Resolution

If another audio output device is connected to the system, Xbox Music, Windows Media Player, Groove Music, or Movies & TV will switch to that audio device when the monitor is powered off and then back to the monitor when the monitor is powered back on. No error messages will be displayed.

To resume playback if no other audio devices are connected to the system when the monitor is powered off, you should open a different audio file or reopen the original audio file after the error message is displayed.

Removing, uninstalling, or reinstalling Microsoft Store app isn't supported

Article • 09/23/2021 • 2 minutes to read

In Windows 10, we don't recommend removing or uninstalling the Microsoft Store app.

Applies to: Windows 10 - all editions
Original KB number: 4339074

More information

This behavior is by design.

If you uninstalled Microsoft Store by any means and want to reinstall it, the only Microsoft-supported method is to reset or reinstall the operating system. It will reinstall Microsoft Store.

> **ⓘ Important**
>
> - Uninstalling the Microsoft Store app is not supported, and uninstalling it may cause unintended consequences.
> - There is no supported workaround to uninstall or reinstall Microsoft Store.

IT professionals can configure, limit, or block access to Microsoft Store for client computers. See Configure access to Microsoft Store.

Error when you start Microsoft Store apps: This app has been blocked by your system administrator

Article • 12/06/2021 • 2 minutes to read

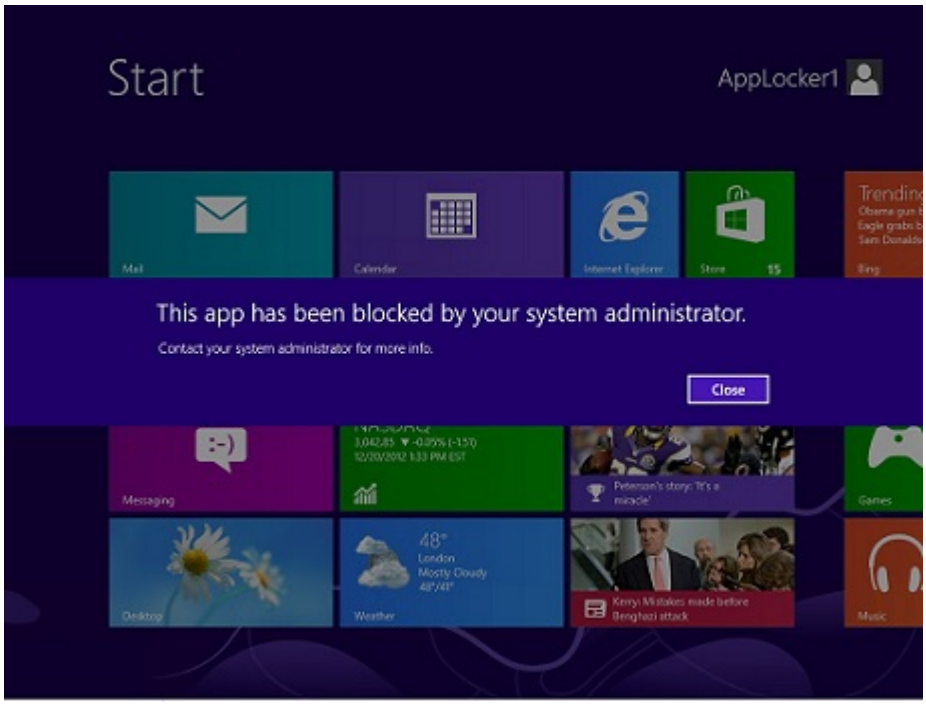
This article helps fix an error (This app has been blocked by your system administrator) that occurs when you to start Microsoft Store apps.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2750770

Symptoms

When you try to start a Microsoft Store app in Windows 8 or in Windows Server 2012, the operation fails. Additionally, you receive the following error message:

> This app has been blocked by your system administrator.



Cause

This issue occurs because an administrator has deployed an application control policy (AppLocker) on the computer. By design, all Microsoft Store apps are blocked if an AppLocker policy is applied.

Resolution

To allow the Microsoft Store app to run, a domain administrator can use AppLocker to edit application control policies. To do so, use one of the following methods, whichever is most appropriate to their situation:

1. Create a default rule that allows all Microsoft Store apps.
2. Create rules that allow individual Microsoft Store apps.

> **Note**
>
> The rules must be edited from a Windows Server 2012-based domain controller or from a Windows 8-based computer that has the Remote Server Administration Tools installed.

More information

For more information about AppLocker, see the following articles:

- AppLocker overview
- Create a rule for packaged apps

Windows Store apps may not open and Event ID 5973 is logged in the Application log

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to fix Event ID 5973 that's logged when Windows Store apps can't be opened.

Applies to: Windows 8.1
Original KB number: 3064045

Symptoms

On a device that is running Windows 8.1, all Windows Store apps do not open and an error that resembles the following is logged in the Application log:

> Log Name: Application
> Source: Microsoft-Windows-Immersive-Shell
> Date: *Date and time*
> Event ID: 5973
> Task Category: (5973)
> Level: Error
> Keywords:
> User: *User ID*
> Computer: *Computer name*
> Description:
> Activation of app *AppID* failed with error: This app does not support the contract specified or is not installed. See the Microsoft-Windows-TWinUI/Operational log for additional information.

Cause

Abnormal shutdown may corrupt the user application cache in `C:\Users\<username>\AppData\Local\Packages`.

Resolution

To test if you have the issue, create a new user account and sign into the new account. If the problem disappears, recreate your user profile to resolve the problem.

1. Back up the user profile data files on the old user account:

    - Swipe in from the right edge of the screen, and then tap Search. (If you're using a mouse, point to the lower-right corner of the screen, move the mouse pointer up, and then click **Search**.)
    - In the **Search** box, type *Show hidden files and folders* and press Enter.
    - In the **Folder Options** dialog, in the **View** tab, look under **Advanced settings**, and set the following settings:
        - **Show hidden files, folders, and drives** button needs to be selected.
        - **Hide extensions for known file types** needs to be unchecked.
        - **Hide protected operating system files (Recommended)** needs to be unchecked.
    - In File Explorer, locate the `C:\Users\Old_Username` folder, where C is the drive that Windows is installed on, and *Old_Username* is the name of the profile you want to back up.
    - Select and copy all of the files and folders in this folder, expect for the following files:
        - NtUser.dat
        - NtUser.ini
        - NtUser.log (or if it does not exist, instead exclude the two log files called ntuser.dat.log1 and ntuser.dat.log2)
    - Paste the files in a backup location of your choosing. You can retrieve your old user account profile from this backup location if needed, however you should be aware that the files that were under `C:\Users\<Old_Username>\AppData\Local\Packages` were likely corrupted, and there may be other files corrupted as well.

2. Sign out of the old user account. If you have e-mail messages in an e-mail program, you must import your e-mail messages and addresses to the new user profile before you delete the old profile. If everything is working properly, you can delete the old profile.

Pre-installed Microsoft Store app is removed unexpectedly at first Windows logon

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for the issue in which a pre-installed Microsoft Store App is unexpectedly removed the first time that a user logs on.

Applies to: Windows 10, version 1903, Windows 10, version 1809
Original KB number: 4543142

Symptoms

You use a DISM command to deploy a Microsoft Store app in Windows 10, version 1809 or a later version of Windows, and then you deploy the app on a computer. After a user logs on to the computer for the first time, the app is unexpectedly removed. Additionally, an Event ID 240 error is generated.

Workaround

To work around this issue, add the `/Region:"All"` switch when you use the DISM command to deploy the app.

Microsoft Store Apps fail to start if default registry or file permissions modified

Article • 09/23/2021 • 10 minutes to read

This article helps fix an issue where you can't start a Microsoft Store App if the default registry or file permissions is modified.

Applies to: Windows 10 - all editions
Original KB number: 2798317

> **Note**
>
> This article is intended for IT professionals. For home users who encounter Microsoft Store App issues, go to **Fix problems with apps from Microsoft Store**.

Issue 1

When you select a Microsoft Store App, the App begins to start, and then Windows just returns to the start screen. No on-screen error is displayed.

Microsoft-Windows-Immersive-Shell event 5961 is logged under the *Applications and Services Logs\Microsoft\Windows\Apps\Microsoft-Windows-TWinUI/Operational event log* path:

Output

```
Log Name:      Microsoft-Windows-TWinUI/Operational
Source:        Microsoft-Windows-Immersive-Shell
Date:          DateTime
Event ID:      5961
Task Category: (5961)
Level:         Error
Keywords:
User:          UserName
Computer:      ComputerName
Description:
Activation of the app <app name> for the Windows.Launch contract failed with
error: The app didn't start.
```

> **Note**

The app portion of the example event, <app name>, will change depending on the application that fails to start.

Possible values for <app name> include but aren't limited to:

> microsoft.windowscommunicationsapps_8wekyb3d8bbwe!Microsoft.WindowsLive.Chat

Prefixes for other built-in Microsoft Store Apps include:

> Microsoft.BingFinance_8wekyb3d8bbwe!<app identifier>
> Microsoft.BingMaps_8wekyb3d8bbwe!<app identifier>
> Microsoft.BingNews_8wekyb3d8bbwe!<app identifier>
> Microsoft.BingSports_8wekyb3d8bbwe!<app identifier>
> Microsoft.BingTravel_8wekyb3d8bbwe!<app identifier>
> Microsoft.BingWeather_8wekyb3d8bbwe!<app identifier>
> Microsoft.Bing_8wekyb3d8bbwe!<app identifier>
> Microsoft.Camera_8wekyb3d8bbwe!<app identifier>
> Microsoft.Media.PlayReadyClient_8wekyb3d8bbwe!<app identifier>
> microsoft.microsoftskydrive_8wekyb3d8bbwe!<app identifier>
> Microsoft.Reader_8wekyb3d8bbwe!<app identifier>
> Microsoft.VCLibs.110.00_8wekyb3d8bbwe!<app identifier>
> microsoft.windows.authhost.a_8wekyb3d8bbwe!<app identifier>
> microsoft.windowscommunicationsapps_8wekyb3d8bbwe!<app identifier>
> microsoft.windowsphotos_8wekyb3d8bbwe!<app identifier>
> Microsoft.WinJS.1.0.RC_8wekyb3d8bbwe!<app identifier>
> Microsoft.WinJS.1.0_8wekyb3d8bbwe!<app identifier>
> Microsoft.XboxLIVEGames_8wekyb3d8bbwe!<app identifier>
> Microsoft.ZuneMusic_8wekyb3d8bbwe!<app identifier>
> Microsoft.ZuneVideo_8wekyb3d8bbwe!<app identifier>

Issue 2

You can't start a Microsoft Store App, open Start screen, and use Search in Windows. Additionally, you receive the following event log in Application logs:

Output

```
Log Name: Application
Source: Application Error
Event ID: 1000
Task Category: (100)
```

```
Level: Error
Keywords: Classic
User: N/A
Description:
Faulting application name: xxxx.exe, version: 10.1605.1606.6002, time stamp:
0x5755acef
Faulting module name: xxxxxx.dll, version: 10.0.14393.1198, time stamp:
0x5902836c
Exception code: 0xc000027b
Fault offset: 0x00000000006d5eab
Faulting process id: 0x29c4
0xc000027b: An application-internal exception has occurred. This error
occurs when an access denied error happens during app initialization that is
fatal and cause an exception that leads to the crash.
```

If you use Process Monitor to track the Apps' executable or related files, you may see **access denied** is logged. It points to the missing permissions for the current logon user. It includes:

1. Registry hives and its subkeys:
   a. HKEY_CLASSES_ROOT
   b. HKEY_LOCAL_MACHINE\Drivers
   c. HKEY_LOCAL_MACHINE\HARDWARE
   d. HKEY_LOCAL_MACHINE\SAM
   e. HKEY_LOCAL_MACHINE\SOFTWARE
   f. HKEY_LOCAL_MACHINE\SYSTEM
   g. HKEY_USERS

2. For file subsystem:
   a. **Program Files** - Read, Read and Execute, and List folder Contents
   b. **Windows** - Read, Read and Execute, and List folder Contents
   c. **Users\<userName>\AppData\Local\Microsoft\Windows\WER** - Special Permissions (List folder/read data, and Create Folders/Append Data)

Cause for issue 1

Registry and or file system permissions may have been changed from their defaults.

The All Application Packages group is a well-known group with a predefined SID. The group must have specific access to certain locations of the registry and file system for Microsoft Store Apps to function properly.

Cause for issue 2

This issue occurs because the read permission is missing from any or all the keys. In this case, **0xc000027b** is logged. This error without exception is missing permission for ALL APPLICATION PACKAGES at registry location or file subsystem locations.

Registry and file system permission must be reverted to a state that will allow Microsoft Store App to function

> **Note**
>
> Only change the permission of the registry keys that are known to cause the access denied error. Incorrectly changing registry keys' permission might cause serious problems or unintentionally weaken security settings.
>
> Extensive permission changes that are propagated throughout the registry and file system cannot be undone. Microsoft will provide commercially reasonable efforts in line with your support contract. However, you cannot currently roll back these changes. We can guarantee only that you can return to the recommended out-of-the-box settings by reformatting the hard disk drive and by reinstalling the operating system.

If you use Group Policy to manage permissions, or if you're unsure whether Group Policy is used to manage permissions, follow these steps:

- Unjoin the computer from the domain or put the computer in a test OU with block policy inheritance enabled. This action prevents the domain-based Group Policy from reapplying the permission changes and breaking the modern applications again after you've fixed them.
- Add permissions where they're required per the following details.
- Edit the Group Policy that manages to permissions so that it no longer breaks modern application.

Registry and File System permission must be reverted back to a state that will allow Microsoft Store App to function. Follow this method to resolve the issue:

1. Determine if file system permissions have been changed. If not, see the More information section below.
2. If so, how were they changed? Manually or with Group Policy?
3. Determine if registry permissions have been changed If not, see the More information section below.

4. If so, how were they changed? Manually or with Group Policy?
5. Verify secpol and GPPs specifically.

Determine if file system permissions have been changed

Check the folders listed below. Determine if the All Application Packages group has the access indicated. Most but not all sub directories of Windows, Program Files, and WER also grant permissions to the All Application Packages group.

- Program Files - Read, Read and Execute, and List folder Contents
- Windows - Read, Read and Execute, and List folder Contents
- Users<userName>\AppData\Local\Microsoft\Windows\WER - Special Permissions (List folder/read data, and Create Folders/Append Data)

Determine if registry permissions have changed

Check the registry keys listed below. Make sure the All Applications Packages group has the Read permissions to the following registry paths:

- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE\Drivers
- HKEY_LOCAL_MACHINE\HARDWARE
- HKEY_LOCAL_MACHINE\SAM
- HKEY_LOCAL_MACHINE\SOFTWARE
- HKEY_LOCAL_MACHINE\SYSTEM
- HKEY_USERS

Most but not all of the subkeys of the registry keys listed above will grant the All Application Packages group read access.

Determine if Group Policy is being used to manage permissions

1. Sign in to a PC as a user experiencing the problem.

2. Open an administrative command prompt then run the following command:

   ```
   Console

   gpresult /h <path>\gpreport.html
   ```

3. Open the file gpreport.html and expand the following path:

Computer Settings > Policies\Windows Settings\Security Settings. Look for **File System** and Registry. If these exist, then GP is assigning permission. You must edit the GP to include the necessary permissions for the All Application Packages group.

Steps to fix the problem

Depending on how the file system permissions were changed will determine how to recover from the problem. The most common ways permissions are changed manually and by Group Policy.

> **ⓘ Important**
>
> Make sure that you test your resolution in a lab before widely deploying. Always backup any important data before changing registry and file system permissions.

Fix file system permissions that's changed manually

1. Open File Explorer.
2. Browse to c:\Program Files.
3. Right click and select **properties**.
4. Select the **Security** tab.
5. Select the **Advanced** button.
6. Select the **Change permissions** button.
7. Select the **Add** button.
8. Select the **Select a principal** link.
9. Select the locations button and select the local computer.
10. Add the All Applications Packages group name and select **ok**.
11. Make sure that Type = allow and Applies to = This folder, subfolder, and files.
12. Check Read & Execute, List folder contents, and Read.
13. Check the **Replace all child object permissions with inheritable permission entries from this object** checkbox.
14. Select **Apply** and **OK**.
15. Repeat for c:\Windows.
16. Repeat for c:\Users but grant the All Application Packages group Full Control.
17. Select **Apply** and **OK**.

Fix file system permissions that's changed by Group Policy

Have a Group Policy administrator do the following steps:

- Open Group Policy Administrative Console.
- Locate the GPO identified in the step Determine if Group Policy is being used to manage permissions.
- Right-click and select **edit**.
- Go to the location Computer `Configuration\Policy\Windows Settings\Security Settings\File System`.
- If there's an entry for the paths already created, you can edit it. If no entry exists, create a new entry for each path.
- To create a new entry, right-click file system and select **add file**.
- Browse to the path c:\Program Files, select **OK**.
- Select the **Add** button.
- Select the locations button and select the local machine name.
- Add the All Application Packages group and grant them the Read, Read and Execute, and List folder Contents permissions.
- Select **Apply** and **OK**.
- Select the **Replace existing permissions on all subfolders and files with inheritable permissions** option.
- Repeat for C:\Windows.
- Repeat for C:\Users, however, grant the All Application Packages group Full Control.

You'll need to wait for the Group policy change to replicate to all Domain Controllers and for all clients to update their Group Policy settings.

> ⓘ **Note**
>
> Processing the File System changes will incur some logon delay the first time this policy is processed. Subsequent logons will not be impacted unless changes are made to the policy. As an alternative you can use a script that is called post logon by the user is run as a scheduled task.

Fix registry permissions that's changed manually

- Open regedit.exe.
- Right click on HKEY_Users and select **properties**.
- Make sure that All Application Packages has Read.
- Repeat for HKEY_CLASSES_ROOT.

- Expand HKEY_LOCAL_MACHINE. Check the subkeys HARDWARE, SAM, SOFTWARE, SYSTEM. Make sure that All Application Packages has the Read permission.

Fix Registry Permissions that's changed by Group Policy

Have a Group Policy administrator do the following steps:

- Open Group Policy Administrative Console.
- Locate the GPO identified in the step Determine if Group Policy is being used to manage permissions.
- Right-click and select **edit**.
- Go to the location Computer `Configuration\Policy\Windows Settings\Security Settings\Registry`.
- Right Click and select **Add Key**.
- Select CLASSES_ROOT.
- Select the **Add** button.
- Select the **locations** button and select the local machine name.
- Add the All Application Packages group and grant them Read.
- Repeat for **Users**.
- Repeat for MACHINE\HARDWARE, MACHINE\SAM, MACHINE\SOFTWARE, and MACHINE\SYSTEM.

More information

For more information, see Microsoft Store Apps Fail to Start if the User Profiles or the ProgramData directory are Moved from their Default Location.

File system and registry access control list modifications

Windows XP and later versions of Windows have tightened permissions throughout the system. So extensive changes to default permissions shouldn't be necessary.

Extra discretionary access control list (DACL) changes may invalidate all or most of the application compatibility testing done by Microsoft. Frequently, changes such as these haven't undergone the thorough testing that Microsoft has done on other settings. Support cases and field experience have shown that DACL edits change the fundamental behavior of the operating system, frequently in unintended ways. These changes affect application compatibility and stability and reduce functionality, about both performance and capability.

Because of these changes, we don't recommend you modify file system DACLs on files that are included with the operating system on production systems. We recommend you evaluate any other ACL changes against a known threat to understand any potential advantages that the changes may lend to a specific configuration. For these reasons, our guides make only minimal DACL changes and only to Windows 2000. For Windows 2000, several minor changes are required. These changes are described in the Windows 2000 Security Hardening Guide.

Extensive permission changes propagated throughout the registry and file system can't be undone. New folders, such as user profile folders that weren't present at the original installation of the operating system, may be affected. So you can't roll back the original DACLs if you:

- remove a Group Policy setting that performs DACL changes
- apply the system defaults

Changes to the DACL in the %SystemDrive% folder may cause the following scenarios:

- The Recycle Bin no longer functions as designed, and files cannot be recovered.
- A reduction of security that lets a non-administrator view the contents of the administrator's Recycle Bin.
- The failure of user profiles to function as expected.
- A reduction of security that provides interactive users with read access to some or to all user profiles on the system.
- Performance problems when many DACL edits are loaded into a Group Policy object that includes long logon times or repeated restarts of the target system.
- Performance problems, including system slowdowns, every 16 hours or so as Group Policy settings are reapplied.
- Application compatibility problems or application crashes.

To help you remove the worst results of such file and registry permissions, Microsoft will provide commercially reasonable efforts in line with your support contract. However, you can't currently roll back these changes. We can guarantee only that you can return to the recommended out-of-the-box settings by reformatting the hard disk drive and by reinstalling the operating system.

For example, modifications to registry DACLs affect large parts of the registry hives and may cause systems to no longer function as expected. Modifying the DACLs on single registry keys poses less of a problem to many systems. We recommend you carefully consider and test these changes before you implement them. And we can guarantee only that you can return to the recommended out-of-the-box settings if you reformat and reinstall the operating system.

Microsoft-Windows-AppReadiness event ID 215 error after a user first logs on

Article • 09/23/2021 • 2 minutes to read

This article explains the Microsoft-Windows-AppReadiness event ID 215 error that occurs after a user first logs on.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 2916750

Symptoms

When a local user logs onto a Windows 8.1 or Windows Server 2012 R2-based computer, a Microsoft-Windows-AppReadiness event ID 215 error is received.

> **Note**
>
> The event log varies slightly, depending on the operating system.

For example, the following event log is received if the computer is running Windows Server 2012 R2:

> Log Name: Microsoft-Windows-AppReadiness/Admin
> Source: Microsoft-Windows-AppReadiness
> Date: **date**
> Event ID: 215
> Task Category: (1)
> Level: Error
> Keywords: (2)
> User: SYSTEM
> Computer: **computer**
> Description: 'ART:ResolveStoreCategories' failed for Administrator. Error: 'Class not registered' (0.015623 second)

The following event log is received if the computer is running Windows 8.1:

> Log Name: Microsoft-Windows-AppReadiness/Admin
> Source: Microsoft-Windows-AppReadiness
> Date: **date**
> Event ID: 215
> Task Category: (1)
> Level: Error
> Keywords: (2)
> User: SYSTEM
> Computer: **computer**
> Description: 'ART:ResolveStoreCategories' failed for Local_Users. Error: 'The network location cannot be reached. For information about network troubleshooting, see Windows Help.' (0.2968801 second)

Cause

The issue occurs because the AppReadiness service queries the Microsoft Store for the category names that are associated with the Microsoft Store Apps installed on the computer when a user logs on for the first time.

The AppReadiness service generates the event logs if the task that obtains the category names fails. A local user account does not have an associated Microsoft account to be used to connect to the Microsoft Store to retrieve the requested data. Therefore, when a local user logs on, the issue that is described in the Symptoms section occurs.

> ⓘ **Note**
>
> The category name is used when you sort Apps by category in the All Apps view of the Start screen. The All Apps view is opened when you click the down arrow button near the bottom of the Start screen.

Resolution

This error can be safely ignored.

Modern apps are blocked by security software when you start the applications on Windows 10

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where modern apps are blocked by security software when you start the applications on Windows 10.

Applies to: Windows 10, version 1903, Windows 10, version 1809, Windows 10, version 1607
Original KB number: 4016973

Symptoms

When you start a Modern app, such as Microsoft.MSN.Money.exe or Microsoft.Photos.exe, on Windows 10, version 1607, Windows 10, version 1809 or Windows 10, version 1903, you notice that the application is blocked by your security software.

Cause

This issue occurs because the individual files within an application package are not digitally signed even though the packages are catalog-signed.

Workaround

To work around this issue, add the affected applications to the allow lists of your security software.

Microsoft Store Apps fail to start if the user profiles or the ProgramData directory are moved from their default location

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where Microsoft Store Apps can't start after the Users directory, a user profile, or the ProgramData directory is moved from their default locations.

Applies to: Windows 10 - all editions
Original KB number: 2787623

Symptoms

After moving the Users directory, an individual user profile, or the ProgramData directory from their default locations, Microsoft Store Apps will no longer start. Various symptoms may be noticed. Some of the symptoms you may see are:

- Clicking the tile for a Microsoft Store App or the Microsoft Store will begin to launch the app but will return to the start screen. No error is displayed.
- Clicking the tile for the Microsoft Store will fail to open the store and return the error:

  > We weren't able to connect to the Store. This might have happened because of a server problem or the network connection timed out. Wait a few minutes and try again. Clicking "try again" may or may not succeed in connecting you to the Store.

- Clicking the tile for the Microsoft Store will open the Store but attempting to purchase apps will return the error:

  > Your purchase couldn't be completed

- The modern PC settings app will not open nor will any of the apps accessed from there.

- The modern Windows Update will not open however the legacy Windows Update accessed via Control Panel will.

Cause

When the Users directory, an individual user profile, or the ProgramData directory is moved to another location other than their default locations, Microsoft Store Apps are no longer supported or expected to work.

Resolution

Don't alter the default location of the USERS directory (c:\users by default) or any individual users profile. Don't alter the default location of the ProgramData directory (c:\ProgramData by default)

More information

Details on the method of relocating the Users and ProgramData directories are located at the links below. These methods are provided as is and intended for test environments only. These methods clearly state that the Microsoft Store and Microsoft Store apps aren't supported if they're used.

- Profilesdirectory
- Programdata

Microsoft Store app cannot start when one user installs an older version than the current version installed by another user in Windows 10

Article • 09/23/2021 • 2 minutes to read

This article provides help to fix an issue where Microsoft Store app cannot start when one user installs an older version than the current version installed by another user.

Applies to: Windows 10 - all editions
Original KB number: 4055744

Symptom

Consider the following scenario:

- On a Windows 10-based computer, you sign in as User A and then install a Microsoft Store app. For example, Minecraft: Education Edition, installed by System Center Configuration Manager as an offline app.
- You update the app to a newer version online from the Microsoft Store, and then sign out as User A.
- You sign in as User B and then install the older version of the app.

In this scenario, you cannot use the app when you sign in as User A. Additionally, when you sign in as User B, you cannot update the app.

This issue can occur when you use System Center Configuration Manager to deploy the older version of an offline app and then the user updates the app online from the Microsoft Store. You will see error 0x3 in the Configuration Manager console when monitoring application status.

Cause

This issue is caused when User B installs the older version of the app and the installation replaces shared files with older versions.

Workaround

The following steps can fix this issue for users on a specific computer:

1. Confirm that the activationStore.dat file does not exist in the AppRepository directory. For example:
   `C:\ProgramData\Microsoft\Windows\AppRepository\Packages\Microsoft.MinecraftEducationEdition_0.21.0_x64__8wekyb3d8bbwe\ActivationStore.dat`

2. Run the following command to set the registry key for the specific application. For example, Minecraft (Microsoft.MinecraftEducationEdition_1.0.21.0_x64__8wekyb3d8bbwe):

   Console

   ```
   reg add
   HKLM\Software\Microsoft\Windows\CurrentVersion\AppModel\StateChange\PackageList\Microsoft.MinecraftEducationEdition_1.0.21.0_x64__8wekyb3d8bbwe /v PackageStatus /t REG_DWORD /d 2
   ```

3. Copy the application.appx file to a local folder, for example: C:\Temp\Microsoft.MinecraftEducationEdition_1.0.21.0_x64__8wekyb3d8bbwe.appx.

4. Set the following command to redeploy the app to run each time that a user signs in. For example, Minecraft (Microsoft.MinecraftEducationEdition_1.0.21.0_x64__8wekyb3d8bbwe):

   PowerShell

   ```
   powershell.exe Add-AppxPackage -Path
   C:\Temp\Microsoft.MinecraftEducationEdition_1.0.21.0_x64__8wekyb3d8bbwe.appx
   ```

   > **Note**
   >
   > If you are using Configuration Manager, do not deploy the app package as a Configuration Manager application.

Resolution

If you are using Configuration Manager, see Manage apps from the Microsoft Store for Business with System Center Configuration Manager to help choose between online or offline app updates.

This issue will not occur in Windows 10 version 1709 and will be fixed for previous versions in an upcoming quality update.

You receive a codec error message, or audio plays but video doesn't play when you play media files in Windows Media Player 11

Article • 09/23/2021 • 4 minutes to read

This article provides a solution to an issue where the video doesn't play when you play it in Windows Media Player 11.

Applies to: Windows Media Player 11
Original KB number: 926373

Symptoms

When you try to play a video file in Windows Media Player 11, the video doesn't play. However, the audio plays.

Additionally, when you try to play an audio file or a video file in Windows Media Player 11, you may receive an error message that resembles one of the following error messages:

> Windows Media Player cannot play the file because the required video codec is not installed on your computer.

> Windows Media Player cannot play, burn, rip, or sync the file because a required audio codec is not installed on your computer.

> A codec is required to play this file. To determine if this codec is available to download from the Web, click Web Help.

> Invalid File Format.

Cause

This problem occurs if a codec that's required to play the file isn't installed on the computer.

Resolution

To resolve this problem, configure Windows Media Player to download codecs automatically. To do so, follow these steps in Windows Media Player 11:

1. On the **Tools** menu, select **Options**.
2. Select the **Player** tab, select the **Download codecs automatically** check box, and then select **OK**.
3. Try to play the file.

If you're prompted to install the codec, select **Install**. If you still can't play the file correctly, try the steps in the **Advanced troubleshooting** section. If you aren't comfortable with advanced troubleshooting, ask someone for help, or contact Microsoft Support.

Advanced troubleshooting

The following steps are intended for advanced computer users.

Obtain and install the codec by following these steps in Windows Media Player 11:

1. Determine whether the codec is installed on the computer that you are using to play the file. To do so, follow these steps:
   a. In the **Now Playing** area, right-click the file that you try to play, and then select **Properties**.
   b. Select the **File** tab, note the codecs that are specified in the **Audio codec** and the **Video codec** areas, and then select **OK**. If the following conditions are true, go to step 2.

      - No audio codec is specified.
      - No video codec is specified.

   c. On the **Help** menu, select **About Windows Media Player**.
   d. Select the **Technical Support Information** hyperlink.
   e. If you're trying to play an audio file, determine whether the audio codec that you noted in step 1b is listed in the **Audio Codecs** area. If you are trying to play a video file, determine whether the video codec or the audio codec that you noted in step 1b is listed in the **Video Codecs** area. If the codec isn't listed, go to step 2.
   f. Try to reinstall the codec. If you can't reinstall the codec, go to step 2.
   g. Try to play the file. If you can play the file, skip steps 2 and 3.

2. Install the codec by following these steps:

a. If you receive an error message when you try to play the file, select **Web Help**. If you don't receive an error message when you try to play the file, go to step 3.

b. On the Microsoft Web site, select the link to the Wmplugins Web site.

c. Follow the instructions on the Web site to download and install the codec for the file. If the Web site doesn't automatically find a codec for the file, and if either of the following conditions is true, go to step 3:

- You didn't note a codec in step 1b.
- You can't find the codec that you noted in step 1b on the Web site.

d. Try to play the file. If you can play the file, skip step 3.

3. Obtain the codec from a third-party vendor.

> ⓘ **Note**
>
> If you are using Windows Media Player in an environment that is managed by a network administrator, you may have to contact the network administrator to download and install the codec.

More information

The information and the solution in this document represents the current view of Microsoft Corporation on these issues as of the date of publication. This solution is available through Microsoft or through a third-party provider. Microsoft doesn't specifically recommend any third-party provider or third-party solution that this article might describe. There might also be other third-party providers or third-party solutions that this article doesn't describe. Because Microsoft must respond to changing market conditions, this information shouldn't be interpreted to be a commitment by Microsoft. Microsoft can't guarantee or endorse the accuracy of any information or of any solution that's presented by Microsoft, or by any mentioned third-party provider.

Microsoft makes no warranties and excludes all representations, warranties, and conditions whether express, implied, or statutory. These include but aren't limited to representations, warranties, or conditions of title, non-infringement, satisfactory condition, merchantability, and fitness for a particular purpose, with regard to any service, solution, product, or any other materials or information. In no event will Microsoft be liable for any third-party solution that this article mentions.

Description of the Windows Media Feature Pack for Windows 7 N and for Windows 7 KN

Article • 09/23/2021 • 6 minutes to read

This article describes the Windows Media Feature Pack for Windows 7 N and for Windows 7 KN.

Applies to: Windows 7 Service Pack 1
Original KB number: 968211

Summary

The N edition and the KN edition of the Windows 7 operating system do not include Windows Media Player or other Windows Media-related technologies, such as Windows Media Center and Windows DVD Maker. Therefore, you must install a separate media player in order to do any of the following:

- Play or create audio CDs, media files, and video DVDs
- Organize content in a media library
- Create playlists
- Convert audio CDs to media files
- View artist and title information about media files
- View album art about music files
- Transfer music to personal music players
- Record and playback TV broadcasts

Additionally, various Web sites and software programs rely on Windows Media-related files that are not incorporated into Windows 7 N and Windows 7 KN. These programs include Microsoft Office and Microsoft Encarta.

To enable all these Web sites and software programs to work correctly, you can install the Windows Media Feature Pack for Windows 7 N and for Windows 7 KN.

More information

Windows 7 N and Windows 7 KN include the same functionality as Windows 7. However, these editions of Windows 7 do not include Windows Media Player or other

Windows Media-related technologies. The programs that are not included in these editions of Windows 7 include the following:

- Windows Media Player User Experience: This feature enables Windows Media Player components, and lets you perform the following actions:
  - Play media files and audio CDs
  - Manage media in a library
  - Create a playlist
  - Provide metadata (including album art) for media
  - Create an audio CD
  - Transfer music to a portable music player
  - Play streamed content from the Web
- Windows Media Player ActiveX Control: This feature exposes methods and properties for manipulating multimedia playback from a Web page or from an application.
- Shell Media Property Display: This feature enables the display of metadata such as artist, song, and album information for media files in the Windows user interface, especially in the Music folder.
- Windows Media Player Visualizations: This feature contains visualizations that let you see visual imagery that is synchronized to the sound of the media content as it plays.
- Windows Media Format: This feature provides support for the following components:
  - The Advanced Systems Format (ASF) file container
  - Windows Media audio and video codecs
  - Basic network streaming capability
  - Digital Rights Management (DRM)
- Windows Media Digital Rights Management: This feature enables the secure delivery of protected content for playback on a computer, a portable device, or a network device.
- Windows Media Device Manager: This feature enables communications between an application, the Windows Media DRM system, and portable audio players.
- Media Sharing: This feature enables music, pictures, and videos on the computer to be shared with other computers and devices on the network. Media Sharing also enables the computer to find music, pictures, and videos on the network.

- Media Foundation: This feature provides support for content protection, audio and video quality. Media Foundation also provides interoperability for DRM.
- Windows Portable Devices Infrastructure: This feature communicates with media devices and storage devices that are attached to the computer, including Media Transfer Protocol devices. This system supersedes both Windows Media Device Manager and Windows Image Acquisition. This system lets computers communicate with music players, storage devices, mobile phones, cameras, and other kinds of devices.
- Windows Media Center: This feature lets you access the digital entertainment library on their personal computer or on their television. You can also use the mouse or the Media Center remote control to perform the following actions:
  - View photos in a cinematic slide show
  - Browse their music collection by cover art
  - Easily play DVDs
  - Watch and record their favorite TV showsMedia Center also lets you download movies and watch them in a 10-foot mode on your television.
- Windows DVD Maker: This feature lets you create video DVDs of home movies and photos that can be viewed on DVD players, regardless of geographical region codes. Windows DVD Maker is included in Windows 7 Professional, Windows 7 Enterprise, and Windows 7 Ultimate. DVD Maker is removed from Windows 7 Professional N and KN, Windows 7 Enterprise N and KN, and Windows 7 Ultimate N and KN.
- Sample Ringtone: Media files in the .wma format are removed from Windows 7 N and from Windows 7 KN.
- Sample Media: Sample content for movies, music, and TV is not included in Windows 7 N or in Windows 7 KN.
- **Turn Windows features on or off** user experience: The media playback applications that let a user add or remove Windows DVD Maker, and Windows Media Center are removed.

Impact on other components

The following components were not removed from Windows 7 N and from Windows 7 KN. However, these components are affected by the media programs that were removed from Windows 7 N and from Windows 7 KN.

- HomeGroup: You cannot share integrated media by using streaming features in Windows 7 N or in Windows 7 KN.
- SideShow: This feature does not work in Windows 7 Professional N or in Windows 7 Professional KN. This feature is not included in Windows 7 Starter N or in Windows 7 Starter KN.
- Windows Experience Index: This feature does not work in Windows 7 N or in Windows 7 KN.
- Windows 7 Games: Games that are included in Windows 7 N and in Windows 7 KN work but do not play back sound effects.
- Windows Mobile Devices: Media synchronization, image acquisition, and file browsing are not supported in Windows 7 N or in Windows 7 KN.
- Windows Photos: Cameras that use the Picture Transfer Protocol (PTP) do not function together with Windows 7 N or with Windows 7 KN.
- Sound Recorder: This feature only records files in the .wav format in Windows 7 N and in Windows 7 KN.
- Group Policy for removable disks: This feature enables computer administrators to set read and write permissions on removable disks. This feature does not work in Windows 7 Professional N or in Windows 7 Professional KN. This feature is not included in Windows 7 Starter N or in Windows 7 Starter KN.
- Microsoft TV Technologies: These do not work in Windows 7 N or in Windows 7 KN.
- MPEG-2 and Dolby Digital Codecs: These codecs are collectively known as "DVD Components." They enable Windows 7 software experiences such as Windows Media Player and Windows Media Center to support activities including the following:
  - DVD playback
  - DVD video burning
  - Television recording and playbackThe MPEG-2 components do not function in Windows 7 N or in Windows 7 KN. These features are not included in Windows 7 Starter N or in Windows 7 Starter KN.
- VC-1, MPEG-4, H.264 codecs: These codecs are collectively known as *standards-based codec* components. They enable Windows 7 software experiences to support various activities. These activities include playing back multimedia files and creating multimedia files. These files are encoded with the standards-based

codecs. The standards-based codec components do not work in Windows 7 N or in Windows 7 KN.

- Windows Premium Sound Schemes: Windows 7 Home Premium and higher editions contain additional sound schemes encoded by using the MP3 codec format. These schemes are not included in Windows 7 N or in Windows 7 KN.
- Sensor and Location Platform: This feature does not work in Windows 7 N or in Windows 7 KN.

For more information about how to download Microsoft support files, see How to obtain Microsoft support files from online services.

Description of Windows Search 4.0 and the Multilingual User Interface Pack for Windows Search 4.0

Article • 09/23/2021 • 5 minutes to read

This article discusses the availability of Windows Search 4.0 and the Multilingual User Interface Pack (MUI) for Windows Search 4.0.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 940157

> **Note**
>
> Support for Windows Vista Service Pack 1 (SP1) ends on July 12, 2011. To continue receiving security updates for Windows, make sure you're running Windows Vista with Service Pack 2 (SP2).

Windows Search 4.0

Windows Search 4.0 lets you perform an instant search of your computer. Windows Search 4.0 helps you find and preview documents, e-mail messages, music files, photos, and other items on the computer.

The search engine in Windows Search 4.0 is a Microsoft Windows service that is also used by programs such as Office Outlook 2007 and Office OneNote 2007. You can use this search engine to index a program's content and to obtain instant results when you search in a particular program.

Windows Search 4.0 includes the following improvements:

- Support for indexing encrypted documents of local file systems
- Reduced effect on Microsoft Exchange when you index e-mail in online mode, and there is no local cache (.ost)
- Support for indexing online delegate mailboxes
- Support forclient-to-client remote query to shared indexed locations
- Improved indexing performance
- Faster previewer updates for Windows XP
- Per-user Group Policy settings
- Windows software updates for Watson errors

- Support for the following new enterprise Group Policy objects:

Computer policies

- Prevent adding Universal Naming Convention (UNC) locations to index from Control Panel
- Prevent customizing indexed locations in Control Panel
- Prevent automatically adding shared folders to the index
- Allow for indexing of encrypted files
- Disable indexer back-off
- Prevent clients from querying the index remotely
- Allow for indexing of online delegate mailboxes
- Prevent adding user-specified locations to the **All Locations** menu
- Enable throttling for online mail indexing

Per-user policies

- Prevent adding UNC locations to the index from Control Panel
- Prevent customizing indexed locations in Control Panel
- Prevent indexing certain paths
- Default indexed paths
- Default excluded paths

Windows Search 4.0 packages include the following:

- The Group Policy template (Search.adm or Search.admx /l) for managing Group Policy objects that span multiple versions of Windows Desktop Search and Windows Search.

- The Add-in for Files on Microsoft Networks for Windows XP and Windows Server 2003 packages.

  This add-in lets Windows Search index redirected *My Documents* folders. This add-in also lets Windows Search index shared items on remote networks. By default, this add-in is included for supported 32-bit operating systems.

When you install the Windows Search 4.0 packages, you also install the following items:

- XmlLite
- IFilters

Windows Search 4.0 supports the following operating systems:

- 32-bit versions of Windows Vista with Service Pack 1 (SP1)
- 64-bit versions of Windows Vista with SP1
- 32-bit versions of Windows XP with Service Pack 2 (SP2) or a later version
- 64-bit versions of Windows XP with Service Pack 2 (SP2) or a later version
- 32-bit versions of Windows Server 2003 with SP2
- 64-bit versions of Windows Server 2003 with SP2
- Windows Server 2008
- Windows Home Server

The Windows Search 4.0 installation process automatically upgrades Windows Desktop Search (WDS) 2.6 and later versions of WDS. If you are running a version of WDS that is earlier than WDS 2.6, use the **Add or Remove Programs** tool to remove the earlier version before you install Windows Search 4.0.

> ⓘ **Note**
>
> To install Windows Search 4.0 successfully on a computer that is running Windows XP or Windows Server 2003, Terminal Services must be running on the computer. Also, Terminal Services must be running for Windows Search 4.0 to function correctly. By default, Terminal Services is configured to start automatically. However, it may have been disabled manually or by third-party software. If Terminal Services is disabled, the installation of Windows Search 4.0 will fail with error code 643.

To determine the status of Terminal Services, and start the service if it is disabled, follow these steps:

1. Click **Start**, click **Run**, type *services.msc*, and then press ENTER.
2. Locate Terminal Services.
3. If the **Status** of the service is not set to **Started**, right-click the service, and then click **Properties**.
4. In the **Startup type** list, click **Automatic**, click **Apply**, and then click **Start**.

> ⓘ **Note**
>
> If the installation of Windows Search 4.0 was not successful because Terminal Services was disabled on the computer, you can now restart the installation of Windows Search 4.0.

Microsoft scanned this file for viruses. Microsoft used the most current virus-detection software that was available on the date that the file was posted. The file is stored on

security-enhanced servers that help prevent any unauthorized changes to the file.

For more information about Windows Search, visit the following Microsoft Web site: https://www.microsoft.com/windows/products/winfamily/desktopsearch/default.mspx

The Multilingual User Interface Pack for Windows Search 4.0

The MUI package for Windows XP and for Windows Server 2003 contain an English (EN-US ENU) package installer that also contains resources for the following 30 languages:

- Brazilian Portuguese (pt-BR PTB)
- Bulgarian (bg-BG BGR)
- Chinese - Simplified (zh-CN CHS)
- Chinese - Traditional (zh-TW CHT)
- Croatian (hr-HR HRV)
- Czech (cs-CZ CSY)
- Danish (da-DK DAN)
- Dutch (nl-NL NLD)
- Estonian (et-EE ETI)
- Finnish (fi-FI FIN)
- French (fr-FR FRA)
- German (de-DE DEU)
- Greek (el-GR ELL)
- Hungarian (hu-HU HUN)
- Italian (it-IT ITA)
- Japanese (ja-JP JPN)
- Korean (ko-KR KOR)
- Latvian (lv-LV LVI)
- Lithuanian (lt-LT LTH)
- Norwegian - Bokmål (nb-NO NOR)
- Polish (pl-PL PLK)
- Portuguese (pt-PT PTG)
- Romanian (ro-RO ROM)
- Russian (ru-RU RUS)
- Slovak (sk-SK SKY)
- Slovenian (sl-SI SLV)
- Spanish (es-ES ESN)
- Swedish (sv-SE SVE)
- Thai (th-TH THA)

- Turkish (tr-TR TRK)

The Windows Search 4.0 MUI installation process automatically upgrades the earlier versions of the WDS 2.6 MUI and later versions of the WDS MUI. If you have an English version of Windows and the Windows MUI and if you have an earlier version of WDS that was a stand-alone non-English installation, use the **Add or Remove Programs** tool to remove the earlier version before you install the Windows Search 4.0 MUI.

> **Note**
>
> The MUI for Windows Server 2003 and Windows XP contains resources for 30 languages.

For more information about how to download Microsoft support files, see How to obtain Microsoft support files from online services.

Microsoft scanned this file for viruses. Microsoft used the most current virus-detection software that was available on the date that the file was posted. The file is stored on security-enhanced servers that help prevent any unauthorized changes to the file.

Troubleshoot kiosk mode issues

Article • 09/02/2022 • 2 minutes to read

Applies to: Windows 10, Windows 11

Single-app kiosk issues

> **Tip**
>
> We recommend that you **enable logging for kiosk issues**. For some failures, events are only captured once. If you enable logging after an issue occurs with your kiosk, the logs may not capture those one-time events. In that case, prepare a new kiosk environment (such as a **virtual machine (VM)**), set up your kiosk account and configuration, and try to reproduce the problem.

Sign-in issues

1. Verify that User Account Control (UAC) is turned on.
2. Check the Event Viewer logs for sign-in issues under *Applications and Services Logs\Microsoft\Windows\Authentication User Interface\Operational*.

Automatic logon issues

Check the Event Viewer logs for auto logon issues under *Applications and Services Logs\Microsoft\Windows\Authentication User Interface\Operational*.

Multi-app kiosk issues

> **Note**
>
> Currently, multi-app kiosk is only supported on Windows 10. It's not supported on Windows 11.

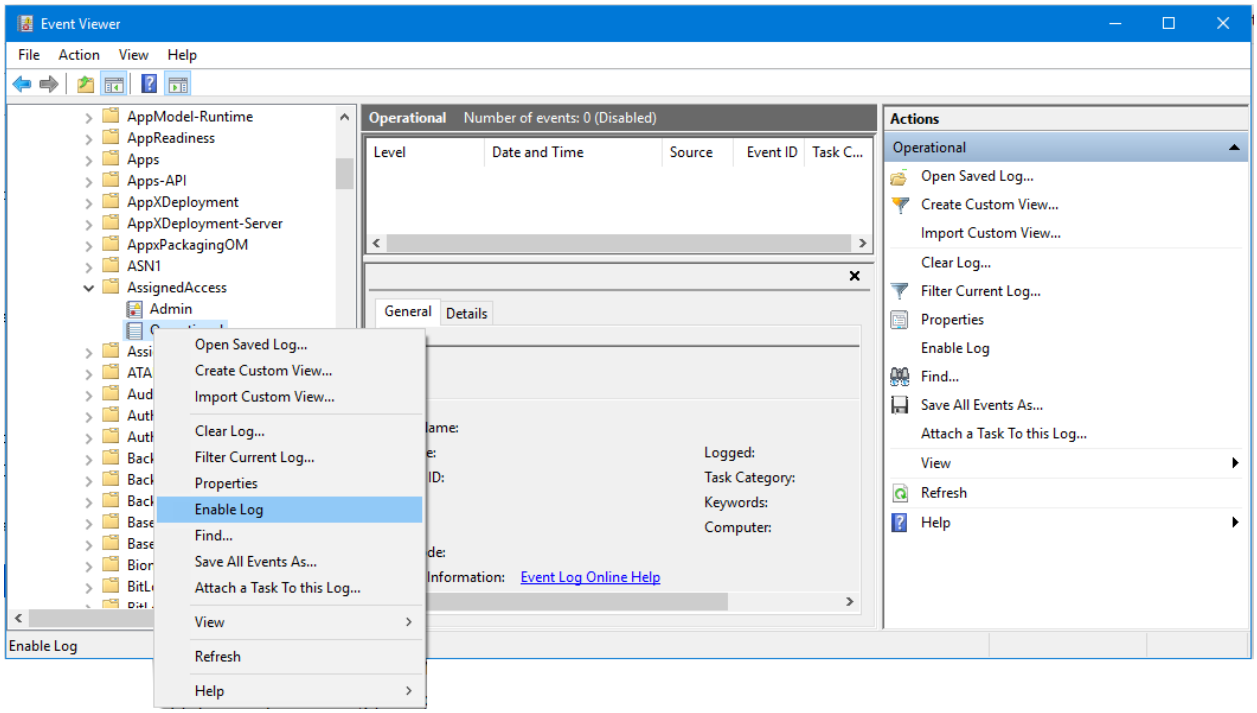
Unexpected results

For example:

- Start isn't launched in full-screen
- Blocked hotkeys are allowed
- Task Manager, Cortana, or Settings can be launched
- Start layout has more apps than expected

Troubleshooting steps

1. Verify that the provisioning package is applied successfully.
2. Verify that the account (config) is mapped to a profile in the configuration XML file.
3. Verify that the configuration XML file is authored and formatted correctly. Correct any configuration errors, then create and apply a new provisioning package. Sign out and sign in again to check the new configuration.
4. Additional logs about configuration and runtime issues can be obtained by enabling the *Applications and Services Logs\Microsoft\Windows\AssignedAccess\Operational* channel, which is disabled by default.



Automatic logon issues

Check the Event Viewer logs for auto logon issues under *Applications and Services Logs\Microsoft\Windows\Authentication User Interface\Operational*.

Apps configured in AllowedList are blocked

1. Ensure the account is mapped to the correct profile and that the apps are specific for that profile.

2. Check the EventViewer logs for Applocker and AppxDeployment (under *Application and Services Logs\Microsoft\Windows*).

Start layout not as expected

- Make sure the Start layout is authored correctly. Ensure that the attributes **Size**, **Row**, and **Column** are specified for each application and are valid.
- Check if the apps included in the Start layout are installed for the assigned access user.
- Check if the shortcut exists on the target device, if a desktop app is missing on Start.

Start menu troubleshooting guidance

Article • 01/22/2023 • 13 minutes to read

Applies to: Windows 10

Start failures can be organized into these categories:

- Deployment/Install issues - Easiest to identify but difficult to recover. This failure is consistent and usually permanent. Reset, restore from backup, or rollback to recover.
- Performance issues - More common with older hardware, low-powered machines. Symptoms include: High CPU utilization, disk contention, memory resources. This makes Start slow to respond. Behavior is intermittent depending on available resources.
- Crashes - Also easy to identify. Crashes in Shell Experience Host or related can be found in System or Application event logs. This can be a code defect or related to missing or altered permissions to files or registry keys by a program or incorrect security tightening configurations. Determining permissions issues can be time consuming but a SysInternals tool called Procmon will show **Access Denied**. The other option is to get a dump of the process when it crashes and depending on comfort level, review the dump in the debugger, or have support review the data.
- Hangs - in Shell Experience host or related. These are the hardest issues to identify as there are few events logged, but behavior is typically intermittent or recovers with a reboot. If a background application or service hangs, Start won't have resources to respond in time. Clean boot may help identify if the issue is related to additional software. Procmon is also useful in this scenario.
- Other issues - Customization, domain policies, deployment issues.

Basic troubleshooting

When troubleshooting basic Start issues (and for the most part, all other Windows apps), there are a few things to check if they aren't working as expected. For issues where the Start menu or subcomponent isn't working, you can do some quick tests to narrow down where the issue may reside.

Check the OS and update version

- Is the system running the latest Feature and Cumulative Monthly update?
- Did the issue start immediately after an update? Ways to check:
  - PowerShell:[System.Environment]::OSVersion.Version

- WinVer from CMD.exe

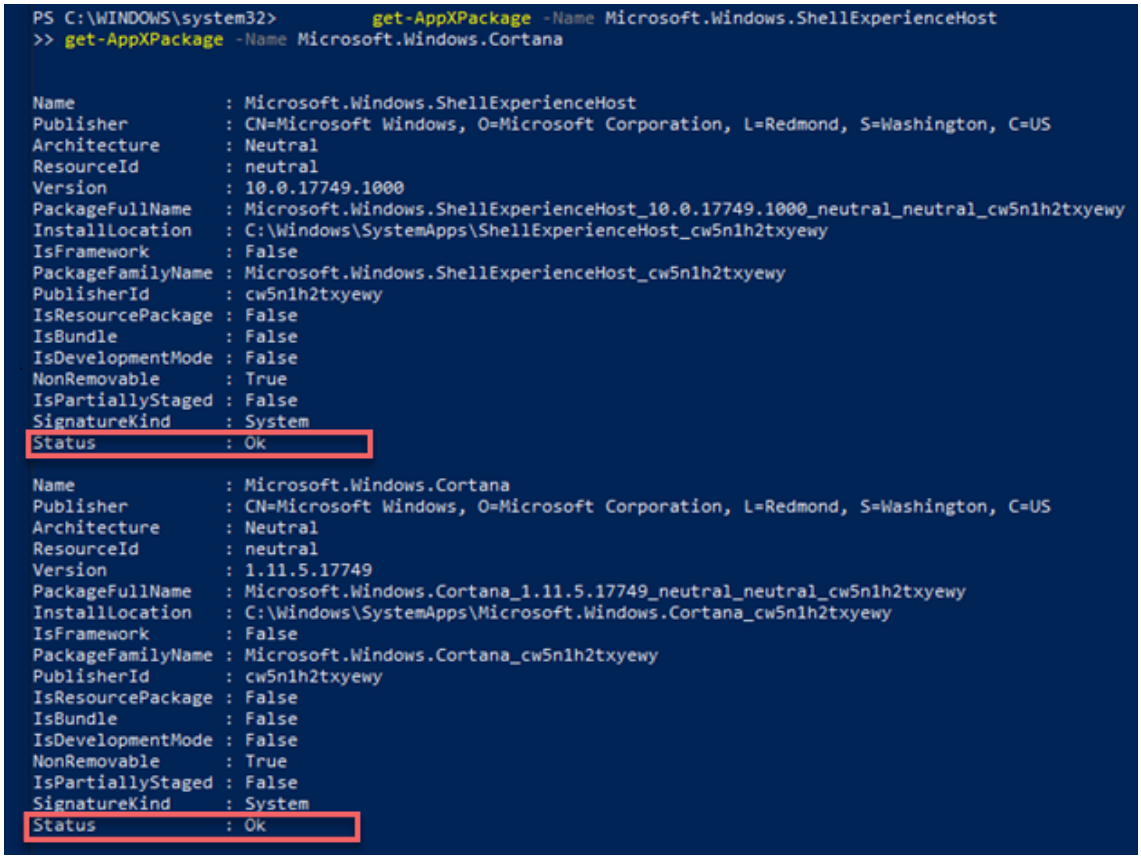
Check if Start is installed

- If Start fails immediately after a feature update, on thing to check is if the App package failed to install successfully.
- If Start was working and just fails intermittently, it's likely that Start is installed correctly, but the issue occurs downstream. The way to check for this problem is to look for output from these two PowerShell commands:
  - PowerShell

    ```
    get-AppXPackage -Name Microsoft.Windows.ShellExperienceHost
    ```

  - PowerShell

    ```
    get-AppXPackage -Name Microsoft.Windows.Cortana
    ```

    Failure messages will appear if they aren't installed

- If Start isn't installed, then the fastest resolution is to revert to a known good configuration. This can be rolling back the update, resetting the PC to defaults (where there's a choice to save to delete user data), or restoring from backup. No

method is supported to install Start Appx files. The results are often problematic and unreliable.

Check if Start is running

If either component is failing to start on boot, reviewing the event logs for errors or crashes during boot may pin point the problem. Booting with MSCONFIG and using a selective or diagnostic startup option will eliminate and/or identify possible interference from additional applications.

- PowerShell

```
get-process -name shellexperiencehost
```

- PowerShell

```
get-process -name searchui
```

If it's installed but not running, test booting into safe mode or use MSCONFIG to eliminate third-party or additional drivers and applications.

Check whether the system a clean install or upgrade

- Is this system an upgrade or clean install?
  - Run `test-path "$env:windir\panther\miglog.xml"`
  - If that file doesn't exist, the system is a clean install.
- Upgrade issues can be found by running `test-path "$env:windir\panther\miglog.xml"`

Check if Start is registered or activated

- Export the following Event log to CSV and do a keyword search in a text editor or spreadsheet:
  - Microsoft-Windows-TWinUI/Operational for Microsoft.Windows.ShellExperienceHost or Microsoft.Windows.Cortana
    - "Package was not found"
    - "Invalid value for registry"
    - "Element not found"
    - "Package could not be registered"

If these events are found, Start isn't activated correctly. Each event will have more detail in the description and should be investigated further. Event messages can vary.

Other things to consider

When did the problem start?

- Top issues for Start menu failure are triggered
  - After an update
  - After installation of an application
  - After joining a domain or applying a domain policy
- Many of those issues are found to be
  - Permission changes on Registry keys or folders
  - Start or related component crashes or hangs
  - Customization failure

To narrow down the problem further, it's good to note:

- What is the install background?
  - Was this a deployment, install from media, other
  - Using customizations?
    - DISM
    - Group Policy or MDM
    - copyprofile
    - Sysprep
    - Other

- Domain-joined
  - Group policy settings that restrict access or permissions to folders or registry keys can cause issues with Start performance.
  - Some Group Policies intended for Windows 7 or older have been known to cause issues with Start
  - Untested Start Menu customizations can cause unexpected behavior by typically not complete Start failures.

- Is the environment virtualized?
  - VMware
  - Citrix
  - Other

Check Event logs that record Start Issues:

- System Event log
- Application Event log
- Microsoft/Windows/Shell-Core*
- Microsoft/Windows/Apps/
- Microsoft-Windows-TWinUI*
- Microsoft/Windows/AppReadiness*
- Microsoft/Windows/AppXDeployment*
- Microsoft-Windows-PushNotification-Platform/Operational
- Microsoft-Windows-CoreApplication/Operational
- Microsoft-Windows-ShellCommon-StartLayoutPopulation*
- Microsoft-Windows-CloudStore*
- Check for crashes that may be related to Start (explorer.exe, taskbar, and so on)
  - Application log event 1000, 1001
  - Check WER reports
    - C:\ProgramData\Microsoft\Windows\WER\ReportArchive\
    - C:\ProgramData\Micrt\Windowsosof\WER\ReportQueue\

If there is a component of Start that is consistently crashing, capture a dump that can be reviewed by Microsoft Support.

Common errors and mitigation

The following list provides information about common errors you might run into with Start Menu, as well as steps to help you mitigate them.

Symptom: Start Menu and other shell components fail when Apps including Barco's ClickShare access Office APIs

You may experience various issues related to the Windows Shell on devices that are running Office ClickToRun, along with some third party applications that use Office APIs:

- Event 1000 is logged in the Application event log. The event log reports that an application crashes for StartMenuExperienceHost.exe, ShellExperienceHost.exe, SearchUI.exe, with an error code 0xc000027b / -1073741189.

- Errors in the Microsoft-Windows-AppModel-State event log mentioning the following error with various package names:

  > Triggered repair of state locations because operation SettingsInitialize against package Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy hit error -2147024891.

- The Windows Start Menu does not respond to mouse clicks or the Windows key.
- Windows Search does not respond to mouse clicks on pressing the Search button or Windows+S key.

Cause

This may occur when a third party process such as ClickShare uses Office APIs on a computer where Office is deployed by using Office ClickToRun. Application packages' permissions are being removed from the following Registry path:

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`

Workaround

1. Download the scripts to fix the issue when it happens, though the scripts cannot prevent the issue from re-occurring.
2. Open a Powershell prompt under the affected user identity, and run

```PowerShell
.\FixUserShellFolderPermissions.ps1
```

- If the script can't access the registry key because the registry permissions are wiped out, then open an elevated Powershell prompt and run the following command:
  - ```PowerShell
    FixUserShellFolderPermissions.ps1 -allprofiles
    ```
- If an application doesn't work, you may need to register the shell packages by running from the affected user the command
  - ```PowerShell
    ```

```
FixUserShellFolderPermissions.ps1 -register
```

> **Note**
>
> If Barco ClickShare v4.27.0.x is installed, either rollback, uninstall or upgrade to stop the propagation. Refer Barco's Knowledge Base, **Unresponsive Windows taskbar or user shell folder permissions issues with ClickShare App Calendar integration**.

Prevent the issue from reoccurring

- In the case of ClickShare, ensure ClickShare v4.27.0.x is not running and then disabling calendar integration would prevent the issue from re-occurring.
- Prevent the applications from running at startup or configure the applications to Start on-demand.

Status

Microsoft is aware of this issue and is working to resolve it. We will post more information in this article when it becomes available.

Symptom: Start Menu doesn't respond on Windows 2012 R2, Windows 10, or Windows 2016

Cause

Background Tasks Infrastructure Service (BrokerInfrastructure) service isn't started.

Resolution

Ensure that Background Tasks Infrastructure Service is set to automatic startup in Services MMC.

If Background Tasks Infrastructure Service fails to start, verify that the Power Dependency Coordinator Driver (PDC) driver and registry key aren't disabled or deleted. If either are missing, restore from backup or the installation media.

To verify the PDC Service, run `C:\>sc query pdc` in a command prompt. The results will be similar to the following:

Output

```
SERVICE_NAME: pdc
TYPE          : 1 KERNEL_DRIVER
STATE          : 4 RUNNING
  (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
WIN32_EXIT_CODE     : 0 (0x0)
SERVICE_EXIT_CODE    : 0 (0x0)
CHECKPOINT       : 0x0
WAIT_HINT        : 0x0
```

The PDC service uses pdc.sys located in the *%WinDir%\system32\drivers*.

The PDC registry key is: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\pdc`
Description="@%SystemRoot%\system32\drivers\pdc.sys,-101"
DisplayName="@%SystemRoot%\system32\drivers\pdc.sys,-100"
ErrorControl=dword:00000003 Group="Boot Bus Extender"
ImagePath=hex(2):73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,64,00,
72,00,69,00,76,00,65,00,72,00,73,00,5c,00,70,00,64,00,63,00,2e,00,73,00,79,
00,73,00,00,00
Start=dword:00000000
Type=dword:00000001

In addition to the listed dependencies for the service, Background Tasks Infrastructure Service requires the Power Dependency Coordinator Driver to be loaded. If the PDC doesn't load at boot, Background Tasks Infrastructure Service will fail and affect Start Menu.

Events for both PDC and Background Tasks Infrastructure Service will be recorded in the event logs. PDC shouldn't be disabled or deleted. BrokerInfrastructure is an automatic service. This Service is required for all these operating Systems as running to have a stable Start Menu.

> ⓘ **Note**
>
> You cannot stop this automatic service when machine is running (*C:\windows\system32\svchost.exe -k DcomLaunch -p*).

Symptom: After upgrading from 1511 to 1607 versions of Windows, the Group Policy "Remove All Programs list from the Start Menu" may not work

Cause

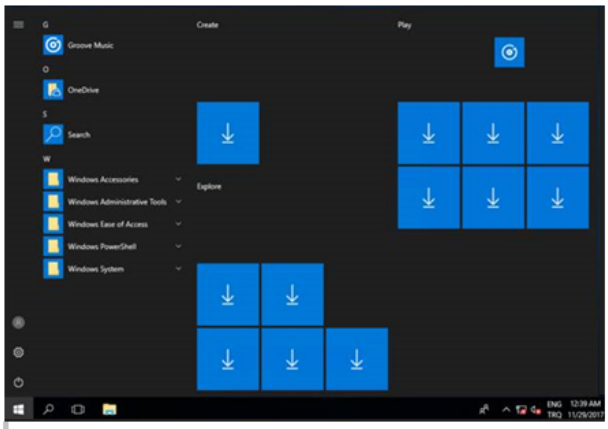
There was a change in the All Apps list between Windows 10, versions 1511 and 1607. These changes mean the original Group Policy and corresponding registry key no longer apply.

Resolution

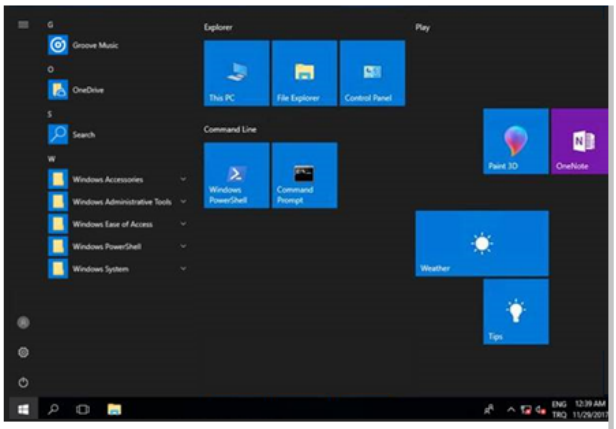
This issue was resolved in the June 2017 updates. Update Windows 10, version 1607, to the latest cumulative or feature updates.

> ⓘ **Note**
>
> When the Group Policy is enabled, the desired behavior also needs to be selected. By default, it is set to **None**.

Symptom: Application tiles like Alarm, Calculator, and Edge are missing from Start menu and the Settings app fails to open on Windows 10, version 1709 when a local user profile is deleted



Download icons on app tiles



Missing app tiles

Cause

This issue is known. The first-time sign-in experience isn't detected and does not trigger the install of some apps.

Resolution

This issue has been fixed for Windows 10, version 1709 in KB 4089848 March 22, 2018—KB4089848 (OS Build 16299.334)

Symptom: When attempting to customize Start Menu layout, the customizations do not apply or results are not expected

Cause

There are two main reasons for this issue:

- Incorrect format: Editing the xml file incorrectly by adding an extra space or spaces, entering a bad character, or saving in the wrong format.
  - To tell if the format is incorrect, check for "Event ID: 22" in the "*Applications and Services\Microsoft\Windows\ShellCommon-StartLayoutPopulation\Operational*" log.
  - Event ID 22 is logged when the xml is malformed, meaning the specified file simply isn't valid xml.
  - When editing the xml file, it should be saved in UTF-8 format.
- Unexpected information: This occurs when possibly trying to add a tile via an unexpected or undocumented method.
  - "Event ID: 64" is logged when the xml is valid but has unexpected values.
  - For example: The following error occurred while parsing a layout xml file:

    > The attribute 'LayoutCustomizationRestrictiontype' on the element '{http://schemas.microsoft.com/Start/2014/LayoutModification}DefaultLayoutOverride' is not defined in the DTD/Schema.

XML files can and should be tested locally on a Hyper-V or other virtual machine before deployment or application by Group Policy

Symptom: Start menu no longer works after a PC is refreshed using F12 during startup

Description

If a user is having problems with a PC, it can be refreshed, reset, or restored. Refreshing the PC is a beneficial option because it maintains personal files and settings. When users have trouble starting the PC, "Change PC settings" in Settings isn't accessible. So, to

access the System Refresh, users may use the F12 key at startup. Refreshing the PC finishes, but Start Menu is not accessible.

Cause

This issue is known and was resolved in a cumulative update released August 30, 2018.

Resolution

Install corrective updates; a fix is included in the September 11, 2018-KB4457142 release.

Symptom: The All Apps list is missing from Start menu

Cause

"Remove All Programs list from the Start menu" Group Policy is enabled.

Resolution

Disable the "Remove All Programs list from the Start menu" Group Policy.

Symptom: Tiles are missing from the Start Menu when using Windows 10, version 1703 or older, Windows Server 2016, and Roaming User Profiles with a Start layout

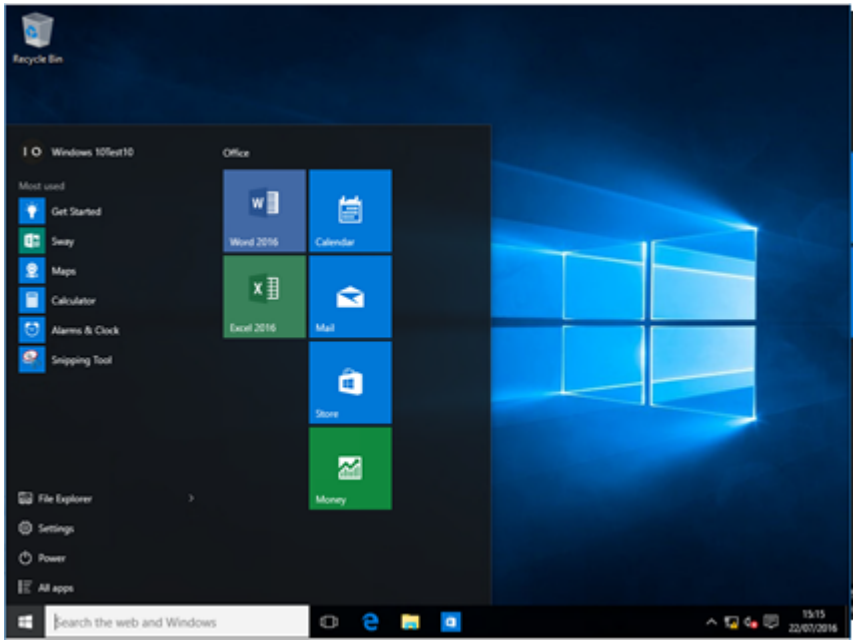
Description

There are two different Start Menu issues in Windows 10:

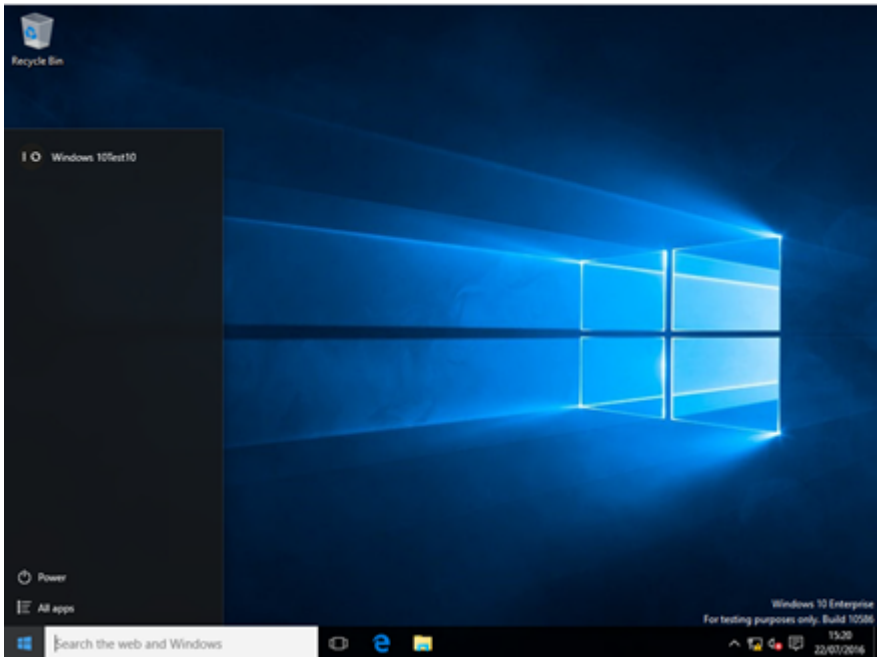
- Administrator configured tiles in the start layout fail to roam.
- User-initiated changes to the start layout are not roamed.

Specifically, behaviors include

- Applications (apps or icons) pinned to the start menu are missing.
- Entire tile window disappears.
- The start button fails to respond.
- If a new roaming user is created, the first sign-in appears normal, but on subsequent sign-ins, tiles are missing.



Working layout on first sign-in of a new roaming user profile



Failing layout on subsequent sign-ins

Cause

A timing issue exists where the Start Menu is ready before the data is pulled locally from the Roaming User Profile. The issue doesn't occur on first logons of a new roaming user, as the code path is different and slower.

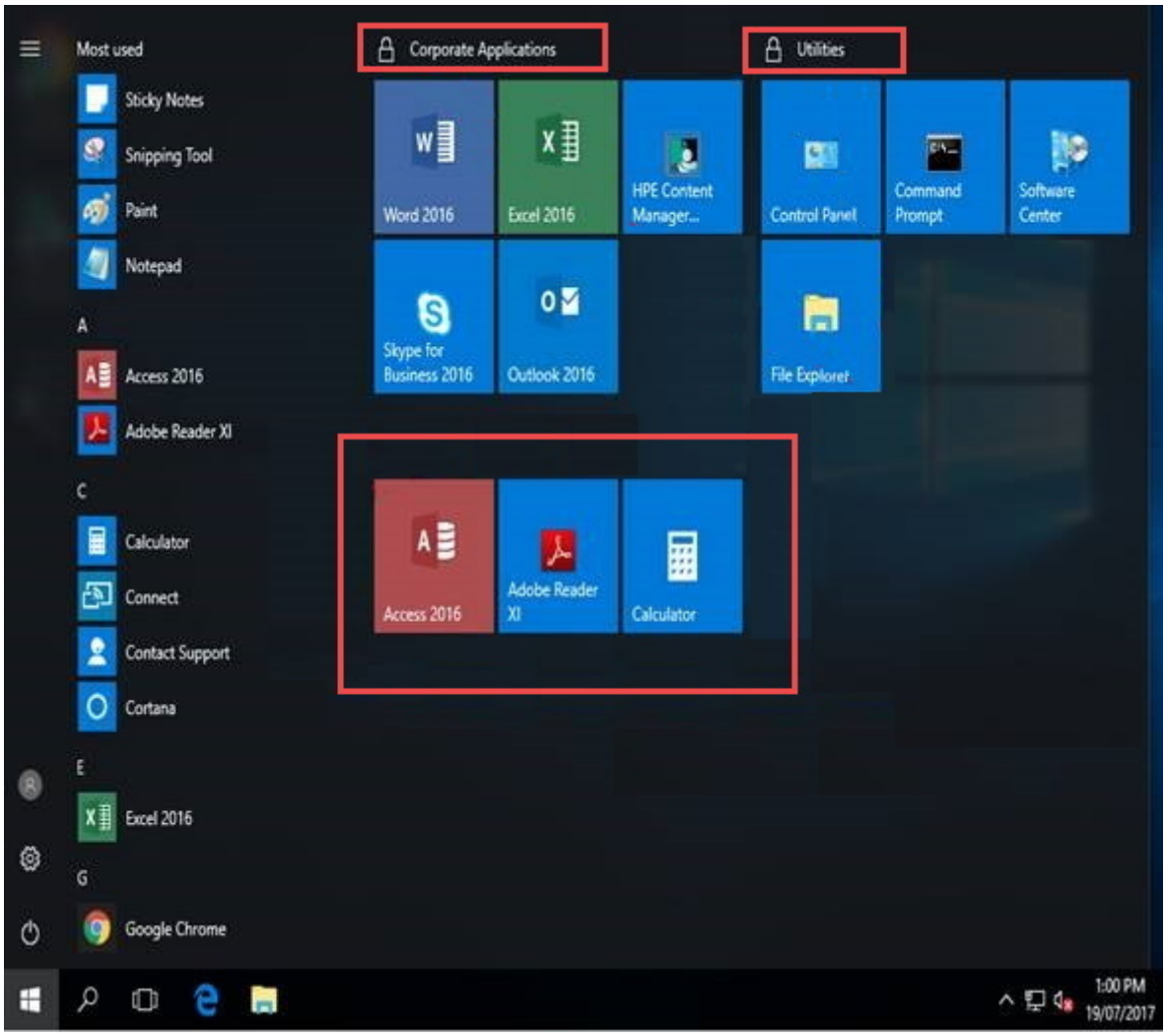
Resolution

This issue has been resolved in Windows 10, versions 1703 and 1607, cumulative updates as of March 2017 .

Symptom: Start Menu layout customizations are lost after upgrading to Windows 10, version 1703

Description

Before the upgrade:

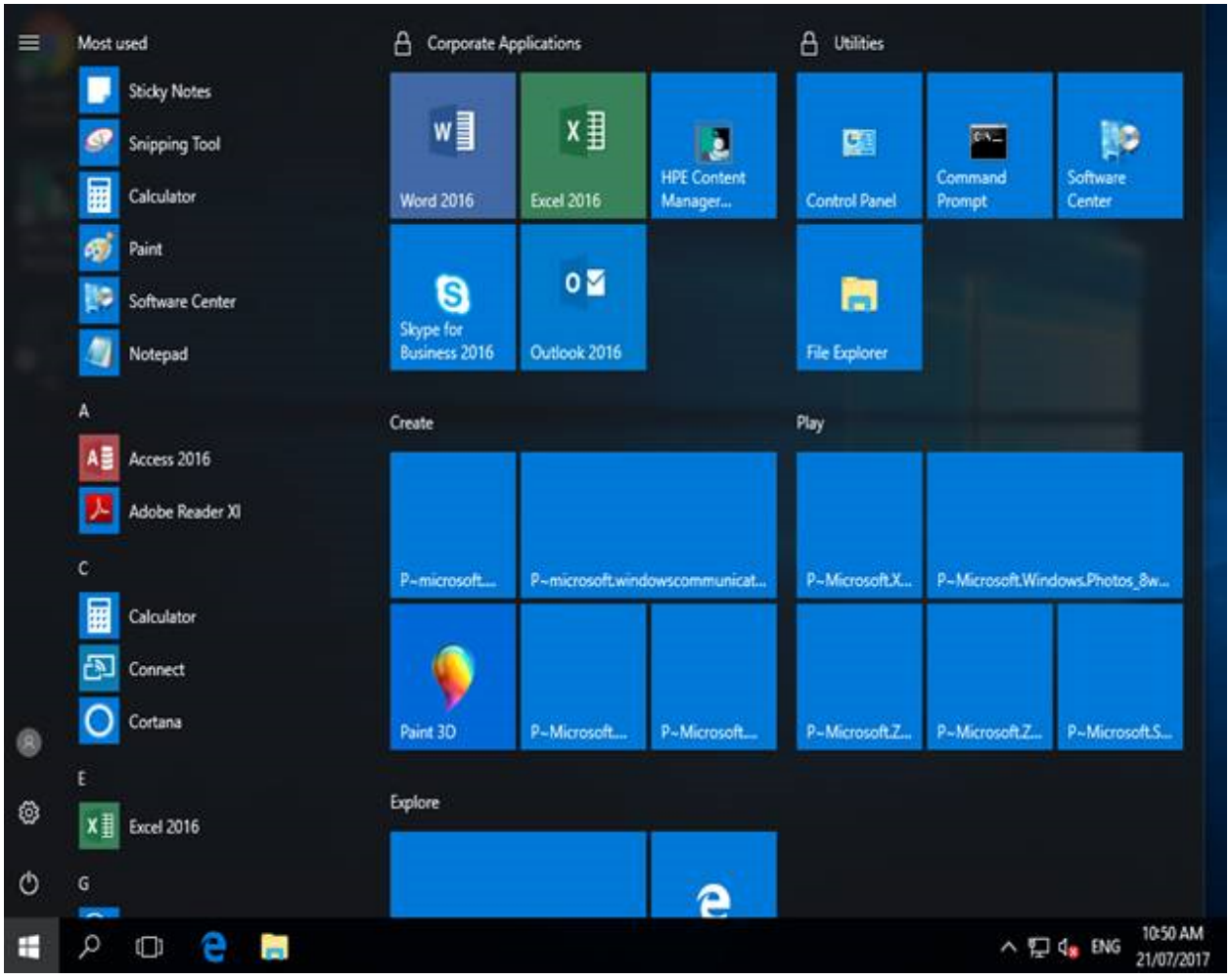


> ⓘ **Note**
>
> In the screenshot, **Corporate Applications** and **Utilities** are group policy controlled, and the tiles under these items are user pinned.

After the upgrade the user pinned tiles are missing:



Additionally, users may see blank tiles if sign-in was attempted without network connectivity.



Resolution

This issue was fixed in the October 2017 update.

Symptom: Tiles are missing after upgrade from Windows 10, version 1607 to version 1709 for users with Roaming User Profiles (RUP) enabled and managed Start Menu layout with partial lockdown

Resolution

The April 2018 LCU must be applied to Windows 10, version 1709 before a user logs on.

Symptom: Start Menu and/or Taskbar layout customizations are not applied if CopyProfile option is used in an answer file during Sysprep

Resolution

CopyProfile is no longer supported when attempting to customize Start Menu or taskbar with a layoutmodification.xml.

Symptom: Start Menu issues with Tile Data Layer corruption

Cause

Windows 10, version 1507 through the release of version 1607 uses a database for the Tile image information. This is called the Tile Data Layer database. (The feature was deprecated in Windows 10 1703.)

Resolution

There are steps you can take to fix the icons, first is to confirm that is the issue that needs to be addressed.

1. The App or Apps work fine when you select the tiles.
2. The tiles are blank, have a generic placeholder icon, have the wrong or strange title information.

3. The app is missing, but listed as installed via PowerShell and works if you launch via URI.
    - Example: `windows-feedback://`
4. In some cases, Start can be blank, and Action Center and Cortana don't launch.

> ⓘ **Note**
>
> Corruption recovery removes any manual pins from Start. Apps should still be visible, but you'll need to re-pin any secondary tiles and/or pin app tiles to the main Start view. Aps that you have installed that are completely missing from "all apps" is unexpected, however. That implies the re-registration didn't work.

Open a command prompt, and run the following command:

```
Console
C:\Windows\System32\tdlrecover.exe -reregister -resetlayout -resetcache
```

Although a reboot isn't required, it may help clear up any residual issues after the command is run.

Symptoms: Start Menu and Apps cannot start after upgrade to Windows 10 version 1809 when Symantec Endpoint Protection is installed

Description

Start menu, Search, and Apps do not start after you upgrade a computer running Windows 7 that has Symantec Endpoint Protection installed to Windows 10 version 1809.

Cause

This problem occurs because of a failure to load *sysfer.dll*. During upgrade, the setup process doesn't set the privilege group "All Application Packages" on *sysfer.dll* and other Symantec modules.

Resolution

This issue was fixed by the Windows Cumulative Update that were released on December 5, 2018—KB4469342 (OS Build 17763.168).

If you've already encountered this issue, use one of the following two options to fix the issue:

Option 1: Remove *sysfer.dll* from system32 folder and copy it back. Windows will set privilege automatically.

Option 2:

1. Locate the directory *C:\Windows\system32*.
2. Right-click on *sysfer.dll* and choose **Properties**.
3. Switch to the **Security** tab.
4. Confirm that **All Application Packages** group is missing.
5. Select **Edit**, and then select **Add** to add the group.
6. Test Start and other Apps.

System Management Components troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve System Management Components-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

System Management Components sub categories

- Event Viewer
- PowerShell
- Server Manager
- Task Scheduler
- WinRM
- WMI

How to delete "Saved Logs" from the Event Viewer

Article • 09/23/2021 • 2 minutes to read

This article describes how to delete files under **Saved Logs** from the Event Viewer.

Applies to: Windows 10 - all editions
Original KB number: 2489761

Symptoms

If you frequently view many EVT or EVTX files in Event Viewer (eventvwr.msc), you may notice a large number of files have accumulated under Saved Logs. These entries are persistent even if the original EVT and EVTX files have been deleted.

Cause

Event viewer stores saved log locations in .XML format. The .XML files can be found in the following directory.
%programdata%\Microsoft\Event Viewer\ExternalLogs

Resolution

The following command can be run from a command prompt to purge the Saved Logs.

```
del /s /q %programdata%\microsoft\eventv~1\extern~1
```

You can also browse to the following location and delete the logs manually:
C:\ProgramData\Microsoft\Event Viewer\ExternalLogs

> ⓘ **Note**
>
> The contents of this folder are hidden so you must turn on **Show Hidden Files** and turn off **Hide Protected Operating System Files** to see them.

More information

Event Viewer reads the saved log locations when it starts and saves them when it is closed. The following actions should be taken to guarantee Saved Logs are deleted

properly.

- Close all instances of Event Viewer (MMC.EXE) before attempting to clear Saved Logs from a command prompt.
- Make sure only one instance of Event Viewer is open if you are manually deleting Saved Logs from the GUI.

Error (MMC has detected an error in a snap-in and will unload it) when you try to launch VAMT 3.0 on a Windows 7 or Windows Server 2008 R2-based computer

Article • 09/23/2021 • 2 minutes to read

This article helps fix an error (MMC has detected an error in a snap-in and will unload it) that occurs when you try to launch the Volume Activation Management Tool (VAMT) 3.0 on a Windows 7 or Windows Server 2008 R2-based computer.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2817142

Symptoms

On a computer that is running Windows 7 or Windows Server 2008 R2, when you try to launch the VAMT 3.0, it may fail. Additionally you may receive the following error message:

> MMC has detected an error in a snap-in and will unload it

You are then prompted with two options:

- Report this error to Microsoft, and then shut down MMC.
- Unload the snap-in and continue running.

If the second option is selected, you may get an error message that is similar to the following:

> Unhandled Exception in Managed Code Snap-in
> FX:{6FBE5D92-C65A-41DC-AEBF-09D8845F68A1}
> Exception has been thrown by the target of an invocation
>
> Exception type:
>
> System.Reflection.TargetInvocationException
>
> Exception stack trace:

at System.RuntimeTypeHandle.CreateInstance(RuntimeType type, Boolean publicOnly, Boolean noCheck, Boolean& canBeCached, RuntimeMethodHandle& ctor, Boolean& bNeedSecurityCheck)
at System.RuntimeType.CreateInstanceSlow(Boolean publicOnly, Boolean fillCache)
at System.RuntimeType.CreateInstanceImpl(Boolean publicOnly, Boolean skipVisibilityChecks, Boolean fillCache)
at System.Activator.CreateInstance(Type type, Boolean nonPublic)
at System.RuntimeType.CreateInstanceImpl(BindingFlags bindingAttr, Binder binder, Object[] args, CultureInfo culture, Object[] activationAttributes)
at System.Activator.CreateInstance(Type type, BindingFlags bindingAttr, Binder binder, Object[] args, CultureInfo culture, Object[] activationAttributes)
at System.Activator.CreateInstance(String assemblyName, String typeName, Boolean ignoreCase, BindingFlags bindingAttr, Binder binder, Object[] args, CultureInfo culture, Object[] activationAttributes, Evidence securityInfo, StackCrawlMark& stackMark)
at System.Activator.CreateInstance(String assemblyName, String typeName)
at System.AppDomain.CreateInstance(String assemblyName, String typeName)
at System.AppDomain.CreateInstanceAndUnwrap(String assemblyName, String typeName)
at Microsoft.ManagementConsole.Internal.SnapInClient.CreateSnapIn(String assemblyName, String typeName)
at Microsoft.ManagementConsole.Internal.ClassLibraryServices.Microsoft.ManagementConsole.Internal.IClassLibraryServices.CreateSnapIn(String assemblyName, String typeName)
at Microsoft.ManagementConsole.Internal.IClassLibraryServices.CreateSnapIn(String assemblyName, String typeName)
at Microsoft.ManagementConsole.Executive.SnapInApplication.CreateSnapIn(String snapInAqn)
at Microsoft.ManagementConsole.Executive.SnapInInitializationOperation.CreateSnapIn()
at Microsoft.ManagementConsole.Executive.Operation.OnThreadTransfer(SimpleOperationCallback callback)

Cause

This problem may occur if you do not have the .NET Framework 3.5.1 feature installed in Windows 7 or Windows Server 2008 R2.

Resolution

To resolve this problem, you need to install .NET Framework 3.5.1 using the following steps:

- On a Windows 7-based computer

    1. Click the **Start** button and then click Control Panel.
    2. Select **Programs**.
    3. Under **Programs and Features**, select **Turn Windows features on or off**.
    4. Select the check box next to the Microsoft .NET Framework 3.5.1.
    5. Click on **OK**.

- On a Windows Server 2008 R2-based computer

    1. Open Server Manager.
    2. Right-click **Features** and select **Add Features**.
    3. Expand **.NET Framework 3.5.1 Features**.
    4. Select the check box next to the .NET Framework 3.5.1
    5. Click on **Install**.

References

- Install and Configure VAMT
- VAMT Requirements
- Install VAMT
- Configure Client Computers

The Windows Trace Session Manager service does not start and Event ID 7000 occurs

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where the Windows Trace Session Manager service doesn't start in the specified time.

Applies to: Windows 10 - all editions
Original KB number: 839803

> **ⓘ Important**
>
> This article contains information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. For information about how to back up, restore, and edit the registry, see **Windows registry information for advanced users**.

Symptoms

The Windows Trace Session Manager service does not start in the timeout value that is specified by Service Control Manager (SCM). By default, the timeout value is 30000 milliseconds (30 seconds).

Additionally, the system event log indicates this timeout failure by a log entry that is similar to the following:

> Source : Service Control Manager
> Event ID : 7000
>
> The Windows Trace Session Manager service failed to start due to the following error:
>
> The service did not respond to the start or control request in a timely fashion.
> For more information, see Help and Support Center at `http://support.microsoft.com`.
> This problem becomes apparent when the installation of Microsoft Enterprise

> Instrumentation Framework (EIF) is not completed. This problem may also become apparent during the computer startup.

Workaround

To work around this problem, increase the default timeout value for the service control manager in the registry.

> **ⓘ Important**
>
> Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall your operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

To increase the timeout value in the registry, follow these steps:

1. Start Registry Editor (Regedit.exe).
2. To change the value data for the ServicesPipeTimeout DWORD value to 60000 in the Control key, follow these steps:
   a. Locate and then click the following registry key:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet`
   b. Click the **Control** subkey.
   c. Right-click the **ServicesPipeTimeout** DWORD value, and then click **Modify**.
   d. Click **Decimal**.
   e. Type *60000*, and then click **OK**.
3. If the **ServicesPipeTimeout** value is *not* available, add the new DWORD value, and then set its value data to 60000 in the Control key. To do so, follow these steps:
   a. Locate and then click the following registry key:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet`
   b. Click the **Control** subkey.
   c. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
   d. Type *ServicesPipeTimeout*, and then press ENTER.

e. Right-click the **ServicesPipeTimeout** DWORD value, and then click **Modify**.

f. Click **Decimal**.

g. Type a value of *60000*, and then click **OK**.

The value is 60000 milliseconds and is equivalent to 60 seconds or to one minute.

> ⓘ **Note**
>
> This change does not take effect until the computer is restarted.

More information

After you increase the ServicesPipeTimeout value in the registry, the service control manager waits for the services to use the whole ServicesPipeTimeout value before the system event log reports that the program did not start.

For services that depend on the Windows Trace Session Manager service and that require several minutes of startup, a value of 60 seconds may not be sufficient time. Therefore, increase the ServicesPipeTimeout value appropriately. This increased value will give all the dependent services sufficient time to start.

Windows PowerShell cmdlet Grant-DfsnAccess doesn't change inheritance on DFS links

Article • 09/20/2022 • 2 minutes to read

This article provides workarounds for an issue where Windows PowerShell cmdlet `Grant-DfsnAccess` doesn't change inheritance on Distributed File System (DFS) links.

Applies to: Windows Server 2016, Windows Server 2012 R2 Standard, Windows 10 - all editions
Original KB number: 2938148

Symptoms

You use the Windows PowerShell cmdlet `Grant-DfsnAccess` to set permissions on DFS links in a DFS namespace in order to have the links filtered by Access Based Enumeration, as in the following example:

PowerShell

```
Grant-DfsnAccess -Path "\\Contoso.com\Software\Projects" -AccountName
"Contoso\UserName"
```

Although the command is completed successfully and the result of the cmdlet shows the correct permissions, you notice that the Access Based Enumeration filtering doesn't reflect the newly set permissions. Additionally, when you check the permissions of the link in the DFS Management Console, you notice that the **Use inherited permission from the local file System** option is still selected.

Cause

Although the `Grant-DfsnAccess` cmdlet successfully configures the view permissions for individual groups or users, the cmdlet doesn't change the inheritance mode from use inherited to set explicit. Therefore, the permissions that are set on the link don't take effect.

Microsoft is aware of this problem with the Windows PowerShell cmdlet `Grant-DfsnAccess`.

Workaround

To work around this problem, use one of the following methods.

- Manually disable inheritance in the DFS Management Console by selecting the **Set explicit view permissions** option.
- Use the `dfsutil property sd grant` command instead, as in the following example:

```
Console

dfsutil property sd grant \\Contoso.com\Software\Projects
Contoso\UserName:RX protect
```

More information

In order to administer DFS namespaces, several Windows PowerShell cmdlets were created as replacement for the command-line utilities such as dfsutil.exe. One of the administrative tasks that is automated is the granting of permissions to DFS links for ABE filtering. By default, DFS namespaces inherit the permission from the DFS root down to the links. This is represented in the Microsoft Management Console (MMC) user interface as use inherited permissions from the local file system. However, for certain links to be displayed while other links aren't, the administrator has to select the **Set explicit view permissions on the DFS folder** option and then set the **Configure View permissions** for the individual users or groups.

Hash of the file does not match when running signed PowerShell script

Article • 09/02/2022 • 2 minutes to read

Applies to: Windows PowerShell

Symptoms

Consider the following scenario:

- You have a PowerShell script that contains special characters like ö, ä, or ü.
- You sign the script on a computer that uses a system locale (for example, en-US).
- You run the signed script on a computer that uses another system locale (for example, cs-CZ).
- The script is encoded with ASCII or UTF-8.

In this scenario, PowerShell displays the following error message:

Output

```
The contents of file <FullPathForSignedPowerShellScript> might have been
changed by an
unauthorized user or process because the hash of the file does not match the
hash stored
in the digital signature. The script cannot run on the specified system.
```

Cause

When you sign the script on an en-US computer, the signing process creates the digital signature for umlaut and special characters by using the en-US code. If you run the signed script on a cs-CZ computer, the signature verification will fail because umlaut and special characters like ö, ä, and ü in ASCII or UTF-8 are encoded differently on en-US and cs-CZ computers.

The signature verification process creates a hash for PowerShell script content that doesn't include the signature. And the umlaut and special characters are interpreted differently on cs-CZ and en-US computers. In this situation, a hash mismatch will occur.

Resolution

To make a signed PowerShell script run independently from locale settings, use one of the following methods:

- Replace or remove all umlaut and special characters like ö, ä, and ü before signing PowerShell scripts.
- Use UTF-16 LE BOM encoding for PowerShell scripts.

More information

For an example (UTF-8 encoded script with special character "ä") that reproduces the issue, see the following steps:

1. You have a computer that has the following settings:

   PowerShell

   ```
   PS C:\Users> get-culture

   LCID             Name             DisplayName
   ----             ----             -----------
   1033             en-US            English (United States)

   PS C:\Users> Get-ExecutionPolicy

   AllSigned

   PS C:\Users> Get-WinSystemLocale

   LCID             Name             DisplayName
   ----             ----             -----------
   1033             en-US            English (United States)
   ```

2. On the same computer, create a PowerShell script *Install.ps1* that contains a special character "ä", and sign the script.

   > **Note**
   >
   > When you run the signed script on the same computer, it works without problems.

3. Run the same signed script on a computer that uses another system locale. For example:

PowerShell

```
PS C:\tmp> Get-Culture

LCID             Name             DisplayName
----             ----             -----------
1033             en-US            English (United States)

PS C:\tmp > Get-ExecutionPolicy

AllSigned

PS C:\tmp > Get-WinSystemLocale

LCID             Name             DisplayName
----             ----             -----------
1029             cs-CZ            Czech (Czech Republic)
```

The script fails with the following messages:

Output

```
File C:\tmp\Install.ps1 cannot be loaded. The contents of file
C:\tmp\Install.ps1 might have been
changed by an unauthorized user or process, because the hash of the
file does not match the hash stored in the digital
signature. The script cannot run on the specified system. For more
information, run Get-Help about_Signing..
At line:1 char:1
+ .\Install.ps1
        + ~~~~~~~~~~~~~
        + CategoryInfo : SecurityError: (:) [], PSSecurityException
        + FullyQualifiedErrorId : UnauthorizedAccess
```

For more information about the PowerShell scripts that are encoded differently, see:

	ASCII encoded PowerShell script	**UTF-8 encoded PowerShell script**	**UTF-16 BE BOM encoded PowerShell script**	**UTF-16 LE BOM encoded PowerShell script**
Windows 10	Affected with HASH mismatch issue	Affected with HASH mismatch issue	n/a (Set-AuthenticodeSignature fails with UnknownError)	NOT affected with HASH mismatch issue
Windows 11	Affected with HASH mismatch issue	Affected with HASH mismatch issue	n/a (Set-AuthenticodeSignature fails with UnknownError)	NOT affected with HASH mismatch issue

	ASCII encoded PowerShell script	UTF-8 encoded PowerShell script	UTF-16 BE BOM encoded PowerShell script	UTF-16 LE BOM encoded PowerShell script
Windows Server 2019	Affected with HASH mismatch issue	Affected with HASH mismatch issue	n/a (Set-AuthenticodeSignature fails with UnknownError)	NOT affected with HASH mismatch issue
Windows Server 2022	Affected with HASH mismatch issue	Affected with HASH mismatch issue	n/a (Set-AuthenticodeSignature fails with UnknownError)	NOT affected with HASH mismatch issue

DNS manager console is missing for RSAT client in Windows 10

Article • 09/23/2021 • 2 minutes to read

This article provides help to solve an issue where DNS server tools are missing after you install the Remote Server Administration Tools for Windows 10 (RSATClient).

Applies to: Windows 10, version 2004, Windows 10, version 1909, Windows 10, version 1803, Windows 10, version 1709
Original KB number: 4055558

Symptom

After you install the RSATClient (WindowsTH-RSAT_WS_1709-x64.msu) by double-clicking the package, the DNS server tools are missing.

This article provides alternative steps to install the RSATClient so that all tools are installed correctly.

Workaround

1. Make sure that update KB 2693643 isn't already installed on the computer. If the update is installed, uninstall the update by using these steps:
   a. Press Win key+R, type *appwiz.cpl* and then press Enter.
   b. Select **View Installed Updates**.
   c. Locate and uninstall the update.
   d. Restart the computer if it prompts.

2. Create a new directory. For example, **temp**.

3. For x64 versions of Windows, create files unattend_x64.xml and installx64.bat. For x86 versions of Windows, create files unattend_x86.xml and installx86.bat.

4. Download the WindowsTH-RSAT_WS_1709-x64.msu package for x64 versions of Windows or the WindowsTH-RSAT_WS_1709-x86.msu package for x86 versions of Windows, and save the package in the new directory.

5. Start a command prompt with administrative permissions and browse to the temp directory.

6. Run installx64.bat for x64 versions of Windows or run installx86.bat for x86 versions of Windows.

> ⓘ **Note**
>
> - After installation, you can clear the contents of the temp directory.
> - No restart is required unless you are prompted.

The installx64.bat file contents

Console

```
@echo off
md ex
expand -f:* WindowsTH-RSAT_WS_1709-x64.msu ex\
cd ex
md ex
copy ..\unattend_x64.xml ex\
expand -f:* WindowsTH-KB2693643-x64.cab ex\
cd ex
dism /online /apply-unattend="unattend_x64.xml"
cd ..\
dism /online /Add-Package /PackagePath:"WindowsTH-KB2693643-x64.cab"
cd ..\
rmdir ex /s /q
```

The unattend_x64.xml file contents

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<unattend xmlns="urn:schemas-microsoft-com:setup" description="Auto
unattend" author="pkgmgr.exe">
    <servicing>
        <package action="stage">
            <assemblyIdentity buildType="release" language="neutral"
name="Microsoft-Windows-RemoteServerAdministrationTools-Client-Package-
TopLevel" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
version="10.0.16299.2"/>
            <source location="." permanence="temporary"/>
        </package>
    </servicing>
</unattend>
```

The installx86.bat file contents

Console

```
@echo off
md ex
expand -f:* WindowsTH-RSAT_WS_1709-x86.msu ex\
cd ex
md ex
copy ..\unattend_x86.xml ex\
expand -f:* WindowsTH-KB2693643-x86.cab ex\
cd ex
dism /online /apply-unattend="unattend_x86.xml"
cd ..\
dism /online /Add-Package /PackagePath:"WindowsTH-KB2693643-x86.cab"
cd ..\
rmdir ex /s /q
```

The unattend_x86.xml file contents

XML

```
<?xml version="1.0" encoding="UTF-8"?>
<unattend xmlns="urn:schemas-microsoft-com:setup" description="Auto
unattend" author="pkgmgr.exe">
    <servicing>
        <package action="stage">
            <assemblyIdentity buildType="release" language="neutral"
name="Microsoft-Windows-RemoteServerAdministrationTools-Client-Package-
TopLevel" processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
version="10.0.16299.2"/>
            <source location="." permanence="temporary"/>
        </package>
    </servicing>
</unattend>
```

Error 0x80041323 when running high number of Scheduled tasks

Article • 09/23/2021 • 3 minutes to read

This article provides a solution to fix the error 0x80041323 that occurs when you run high number of Scheduled tasks.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2696472

Symptoms

Consider the scenario:

- You have a Windows computer that runs high number of Scheduled tasks under one user account.
- The tasks are failing intermittently and under the LastRun option, you may see following error message

  > The task scheduler service is too busy 0x80041323

- Under the Task Scheduler operational log you may see the following event logged:

  > Log Name: Microsoft-Windows-TaskScheduler/Operational
  > Source: Microsoft-Windows-TaskScheduler
  > Event ID: 706
  > Task Category: Compatibility module task status update failed
  > Description: Task Compatibility module failed to update task "<task.job>" to the required status 0. Additional Data: Error Value: 2147942405.
  > The error further implies to:
  >
  > for decimal -2147216605 / hex 0x80041323 SCHED_E_SERVICE_TOO_BUSY
  >
  > The Task Scheduler service is too busy to handle your

- Additionally, you may also notice following events getting logged in Task Scheduler operational log if Task Queue quota or Engine quota exceeded:
- If Task Queue quota exceeded:

> Event ID 131
> Description: Task Scheduler failed to start task "<Task_Name>"; because the number of tasks in the task queue exceeding the quota currently configured to <Task_Queue_Limit>.
> User Action: Reduce the number of running tasks or increase the configured queue quota.
> Event ID 132
> Description: Task Scheduler task launching queue quota is approaching its preset limit of tasks currently configured to <Task_Limit>.
> User Action: Reduce the number of running tasks or increase the configured queue quota.

- If Engine quota exceeded:

> Event ID 133
> Description: Task Scheduler failed to start task <Task_Name> in TaskEngine <Engine_Name> for user <User_Name>.
> User Action: Reduce the number tasks running in the specified user context.
> Event ID 134
> Description: Task Engine <Engine_Name> for user <User_Name> is approaching its preset limit of tasks.
> User Action: Reduce the number of running tasks or increase the configured queue quota.

> **ⓘ Note**
>
> Event ID 132 and Event ID 134 are just an indicator of the approaching issue and not the issue itself. The issue may or may not happen after these events.

Cause

Based on code `SCHED_E_SERVICE_TOO_BUSY`, this is logged when the queue is full. The above issue occurs if:

1. Task Queue quota is exceeded.
2. Engine quota is exceeded.

Resolution

To resolve this particular issue, increase the value for the quota keys to maximum.

> ⊗ **Caution**
>
> This section contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs.

1. Click **Start**, type *regedit*, and then press ENTER.
2. Locate and then click the following registry key:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Schedule\Configuration`
3. Right-click **TasksInMemoryQueue**, click **Edit**, and then click **Modify**.
4. In the **Value data** box, type *1000* (Decimal).
5. Right-click **TasksPerHighestPrivEngine**, click **Edit**, and then click **Modify**.
6. In the **Value data** box, type *1000* (Decimal).
7. Right-click **TasksPerLeastPrivEngine**, click **Edit**, and then click **Modify**.
8. In the **Value data** box, type *1000* (Decimal).
9. Exit **Registry Editor** and reboot the machine.

More information

The Job queue quota is controlled through 'TasksInMemoryQueue' value while the Engine quota is controlled through "TasksPerHighestPrivEngine" and "TasksPerLeastPrivEngine" registry values located under following registry key:

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Schedule\Configuration`

- TasksInMemoryQueue [Default = 75, Max = 1000]
  - Determines the maximum tasks allowed to be queued in the session manager. Once this limit is exceeded, any new task instance scheduled to be executed will be discarded and you'll get the Event ID 131.
  - This queue is shared by all tasks.
- TasksPerHighestPrivEngine [Default = 100, Max = 1000]
  - Determines the maximum number of task instances allowed to be in RUNNING state for an "elevated" task engine (taskeng.exe) at any given point of time.
  - One task engine exists per user session (like SYSTEM, LOCAL SERVICE, Administrator, USER1, USER2 etc.)

    - Here "elevated" corresponds to those tasks that have the option "Run with highest privileges" selected.
- TasksPerLeastPrivEngine [Default = 50, Max = 1000]
    - Similar to "TasksPerHighestPrivEngine" except that it corresponds to non-elevated tasks.

Reference

Event ID 131 - Task Scheduler Service Quotas
Event ID 132 - Task Scheduler Service Quotas

Error when you use the /z switch together with the Schtasks command in Windows Vista: The task XML is missing a required element or attribute

Article • 04/12/2022 • 2 minutes to read

This article helps resolve an issue where you receive an error when you use the **/z** switch together with the **Schtasks.exe** command in Windows Vista.

Applies to: Windows Vista
Original KB number: 2004151

Symptoms

When you use the **/z** switch together with the `Schtasks.exe` command in Windows Vista, you may receive the following error message:

> Error: The task XML is missing a required element or attribute.

The **/z** switch is used to delete a task after it's completed. For example, you can use the following command to start the Calc.exe process at a specified date and time:

```
Console

schtasks /create /tn "calculator" /tr c:\Windows\System32\calc.exe /sc once
/sd 12/02/2010 /st 03:39:00 /z
```

> **Note**
>
> This issue affects only the Schtasks.exe tool. You should be able to use the Scheduled Tasks interface to auto-delete a task after it's completed.

Cause

This issue occurs because of changes in the Task Scheduler service in Windows Vista.

Resolution

To resolve this issue, use the **/V1** switch. The **/V1** switch creates a task that is compatible with pre-Windows Vista platforms. For example, use the following command to start the Calc.exe process at a specified date and time in a pre-Windows Vista environment:

Console

```
schtasks /create /tn "calculator" /tr c:\Windows\System32\calc.exe /sc once
/sd 12/02/2010 /st 03:39:00 /V1 /Z
```

More information

For more information about the **/V1** switch, visit the following MSDN website:

Schtasks.exe

How to run programs automatically when a user logs on

Article • 06/20/2022 • 2 minutes to read

This article describes how to use group policies in Windows 2000 to configure a program to run automatically when a user signs in.

Applies to: Windows 2000
Original KB number: 240791

Summary

You can apply a policy to an individual user or to a computer, and you can use any valid program (custom, third-party, or Windows 2000 programs such as Microsoft Internet Explorer). For example, use the appropriate method to configure Notepad.exe to run when a user signs in:

- To configure Notepad to run when any user signs in to a specific computer:

    1. Edit the following group policy:
       Computer Configuration\Administrative Templates\System\Logon\Run These Programs at User Logon

    2. Type the full path name of the program. In this example, type the following path name:
       `c:\%windir%\system32\notepad.exe`

- To configure Notepad to run when a specific user logs on (regardless of the computer he or she uses):

    1. Edit the following group policy:
       User Configuration\Administrative Templates\System\Run These Programs at User Logon

    2. Type the full path name of the program.

> **Note**
>
> If the program doesn't run, make sure the path is correct. The program doesn't run (and no error message is displayed) if the path isn't found.

Task scheduler task only runs in the background after you use sysprep to create master image

Article • 09/23/2021 • 2 minutes to read

This article provides solutions to an issue where task scheduler runs tasks as background processes after you use sysprep to create the master image.

Applies to: Windows 10 - all editions
Original KB number: 253942

Symptoms

Task scheduler runs tasks as background processes after sysprep-ing the master computer.

After running mini-setup, in end-user mode, any scheduled task that is started through the Windows Task Scheduler never shows up as a window on the desktop.

The Windows Task Manager shows the task as a process but not as an application. For example, if Calc.exe is scheduled by Task Scheduler at 3 P.M., Calc.exe runs at exactly 3 P.M. but does not appear on the desktop. Instead, Calc.exe acts like a background process.

This behavior occurs only if you used SYSPREP to create the master image, and is language independent.

Cause

After running sysprep on the machine, the following registry entry will contain the path to Explorer.exe and a comma at the end of the value: "C:\Winnt\Explorer.exe,"
`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ Shell:REG_SZ:C:\Winnt\Explorer.exe,`

The full path to Explorer.exe, including the command, results in this behavior.

Resolution

The options to resolve this problem are:

Modify the following registry value removing the path to explorer and the trailing comma at the end of explorer as described in the Cause section above. The value should read exactly as shown here: `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ Shell:REG_SZ:Explorer.exe`

-or-

If you are not using SP1 yet, then you should use Sysprep version 1.1 with the -CLEAN switch. To accomplish that task, follow these steps:

1. Add the following to your Sysprep.inf file:

   ```
   INF

   [Unattended]
   InstallFilesPath="%systemdrive%\sysprep\i386"
   ```

   Create the \i386OEM directory structure below the sysprep directory (for example, c:\sysprep\i386OEM)

   or

   drive:\distribution$OEM$$1\sysprep\i386OEM (for a distribution share that already contains Sysprep).

2. Create a Cmdlines.txt file in %systemdrive%\sysprep\i386OEM (or drive:\distribution$OEM$$1\sysprep\i386OEM), which contains the following:

   ```
   INF

   [Commands]
   "%systemdrive%\sysprep\sysprep.exe -clean"
   ```

> ⓘ **Note**
>
> Running sysprep from the audit mode or the [GUIRunOnce] section of the Unattend.txt file is still required. This method ensures that sysprep -CLEAN runs separately during the mini-setup.

Status

Microsoft has confirmed this to be a problem in the Microsoft products listed at the beginning of this article.

More information

Steps to Reproduce Behavior

1. Perform a retail install (can be an unattended installation) of Microsoft Windows 2000.
2. Create the C:\Sysprep folder.
3. Copy the Setupcl.exe, Sysprep.exe, and Sysprep.inf files into the C:\Sysprep folder.
4. Run SYSPREP without any switches.
5. Reboot the system.
6. Follow through the mini-setup wizard.
7. Run Task Scheduler in end user mode and go through the Task Scheduler Wizard.
8. Select an application to schedule (for example, Calc.exe or CDplayer.exe).
9. Select the "One time only" option and specify the date and time for the application to run.
10. Input a user name and password or use the default administrator account.
11. Wait until the specified time.

Use the at command to schedule tasks

Article • 09/23/2021 • 7 minutes to read

This article describes how to use the at command to create and to cancel scheduled tasks.

Applies to: Windows 2000
Original KB number: 313565

> ⓘ **Note**
>
> This article applies to Windows 2000. Support for Windows 2000 ends on July 13, 2010. For more information, see the **Microsoft Support Lifecycle Policy**.

Summary

In Windows 2000, you can use the Task Scheduler tool in Control Panel to schedule tasks. You can also use the at command to schedule tasks manually.

Overview of the at command

You can use the at command to schedule a command, a script, or a program to run at a specified date and time. You can also use this command to view existing scheduled tasks.

To use the at command, the Task Scheduler service must be running, and you must be logged on as a member of the local Administrators group. When you use the at command to create tasks, you must configure the tasks so that they run in the same user account.

The at command uses the following syntax:

- `at \\computername time/interactive | /every: date, ... /next: date, ... command`
- `at \\computername id/delete | /delete /yes`

The following list describes the parameters that you can use with the at command:

- **\computername**: Use this parameter to specify a remote computer. If you omit this parameter, tasks are scheduled to run on the local computer.

- **time**: Use this parameter to specify the time when the task is to run. Time is specified as **hours**: **minutes** based on the 24-hour clock. For example, 0:00 represents midnight and 20:30 represents 8:30 P.M.
- **/interactive**: Use this parameter to allow the task to interact with the desktop of the user who is logged on at the time the task runs.
- /every: **date**,... : Use this parameter to schedule the task to run on the specified day or days of the week or month, for example, every Friday or the eighth day of every month. Specify **date** as one or more days of the week (use the following abbreviations: M,T,W,Th,F,S,Su) or one or more days of the month (use the numbers 1 through 31). Make sure that you use commas to separate multiple date entries. If you omit this parameter, the task is scheduled to run on the current day.
- /next: **date**, ...: Use this parameter to schedule the task to run on the next occurrence of the day (for example, next Monday). Specify **date** as one or more days of the week (use the following abbreviations: M,T,W,Th,F,S,Su) or one or more days of the month (use the numbers 1 through 31). Make sure that you use commas to separate multiple date entries. If you omit this parameter, the task is scheduled to run on the current day.
- **command**: Use this parameter to specify the Windows 2000 command, the program (.exe or .com file), or the batch program (.bat or .cmd file) that you want to run. If the command requires a path as an argument, use the absolute path name (the entire path beginning with the drive letter). If the command is on a remote computer, use the Uniform Naming Convention (UNC) path name (**ServerName*\ **ShareName**). If the command is not an executable (.exe) file, you must precede the command with `cmd /c`, for example, `cmd /c copy C:\*.* C:\temp`.
- **id**: Use this parameter to specify the identification number that is assigned to a scheduled task.
- /delete: Use this parameter to cancel a scheduled task. If you omit the id parameter, all scheduled tasks on the computer are canceled.
- /yes: Use this parameter to force a yes answer to all queries from the system when you cancel scheduled tasks. If you omit this parameter, you are prompted to confirm the cancellation of a task.

> ⓘ **Note**

When you use the at command, the scheduled task is run by using the credentials of the system account.

Create a scheduled task

1. Click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
2. At the command prompt, type the `net start` command, and then press ENTER to display a list of currently running services:

   If Task Scheduler is not displayed in the list, type the following line, and then press ENTER:

   ```
   Console

   net start "task scheduler"
   ```

3. At the command prompt, type the following line (use the parameters that are appropriate to your situation), and then press ENTER:

   ```
   Console

   at \\computername time/interactive | /every: date, ... /next: date, ...
   command
   ```

Examples

- To copy all files from the Documents folder to the MyDocs folder at midnight, type the following line, and then press ENTER:

  ```
  Console

  at 00:00 cmd /c copy C:\Documents\*.* C:\MyDocs
  ```

- To back up the Products server at 11:00 P.M. each weekday, create a batch file that contains the backup commands (for example, Backup.bat), type the following line, and then press ENTER to schedule the backup:

  ```
  Console

  at \\products 23:00 /every:M,T,W,Th,F backup
  ```

- To schedule a net share command to run on the Sales server at 6:00 A.M. and to redirect the listing to the Sales.txt file in the shared Reports folder on the Corp server, type the following line, and then press ENTER:

```
Console

at \\sales 06:00 cmd /c "net share reports=d:\Documents\reports >>
\\corp\reports\sales.txt"
```

Cancel a scheduled task

1. Click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
2. At the command prompt, type the `net start` command, and then press ENTER to display a list of currently running services.

   If Task Scheduler is not displayed in the list, type the following line, and then press ENTER:

```
Console

net start "task scheduler"
```

3. At the command prompt, type the following line (use the parameters that are appropriate to your situation), and then press ENTER:

```
Console

at \\computername id /delete | /delete /yes
```

Examples to cancel scheduled tasks

- To cancel all tasks that are scheduled on the local computer, type `at /delete`, and then press ENTER.
- To cancel the task ID 8 on a computer that is named *MyServer*, type `at \\MyServer 8 /delete`, and then press ENTER.

View scheduled tasks

To view the tasks that you created by using the at command, follow these steps:

1. Click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
2. At the command prompt, type the `net start` command, and then press ENTER to display a list of currently running services.

   If Task Scheduler is not displayed in the list, type the following line, and then press ENTER:

   ```
   Console

   net start "task scheduler"
   ```

3. At the command prompt, do one of the following steps:

   - To view a list of tasks that you scheduled by using the at command, type the `at \\computername` line, and then press ENTER.
   - To view a specific scheduled task, type the `at \\computername id` command, and then press ENTER.

Examples to view scheduled tasks

- To view all scheduled tasks on the local computer, type `at`, and then press ENTER.
- To view all scheduled tasks on a computer named *Support*, type `at \\support`, and then press ENTER.
- To view the task ID 18 on the local computer, type `at 18`, and then press ENTER.

Troubleshooting

- When you type `at \\computername` to view a list of scheduled tasks, some (or all) of the scheduled tasks that you created by using the at command are not listed.

  This behavior can occur if you modified the tasks in the Scheduled Tasks folder after you used the at command to create the task. When you use the at command to schedule a task, the task is displayed in the Scheduled Tasks folder in Control Panel. You can view or modify the task. However, if you modify the task, when you use the at command, you cannot view the task.

- When you use the at command to schedule a task, the task does not run at the specified time or date.

This behavior can occur if one of the following conditions is true:

- The command syntax is incorrect.

  After you schedule a task, type `at \\computername` to confirm that the syntax is correct. If the information that is displayed under Command Line is incorrect, cancel the task, and then recreate it.

- You schedule a task to run a command that is not a .exe file.

The at command does not automatically load cmd (the command interpreter) before it runs commands. Unless you are running a .exe file, you must load Cmd.exe at the beginning of the command, for example, `at cmd /c dir > c:\test.txt`.

References

For more information about how to use the at command in Windows 2000, see Windows 2000 Help. To do so, click **Start**, click **Help**, click the **Index** tab, and then type at command.

Windows Error Reporting and Windows diagnostics enablement guidance

Article • 01/13/2023 • 4 minutes to read

This article provides guidance on Windows Error Reporting (WER) and diagnostic data (Telemetry). WER is an event-based feedback infrastructure designed to collect information on issues that Windows can detect, report the information to Microsoft, and provide users with any available solutions.

Enable Windows Error Reporting (WER)

1. Expand **Policies** under **Computer Configuration** in **Group Policy Management Editor** (*gpmc.msc*).

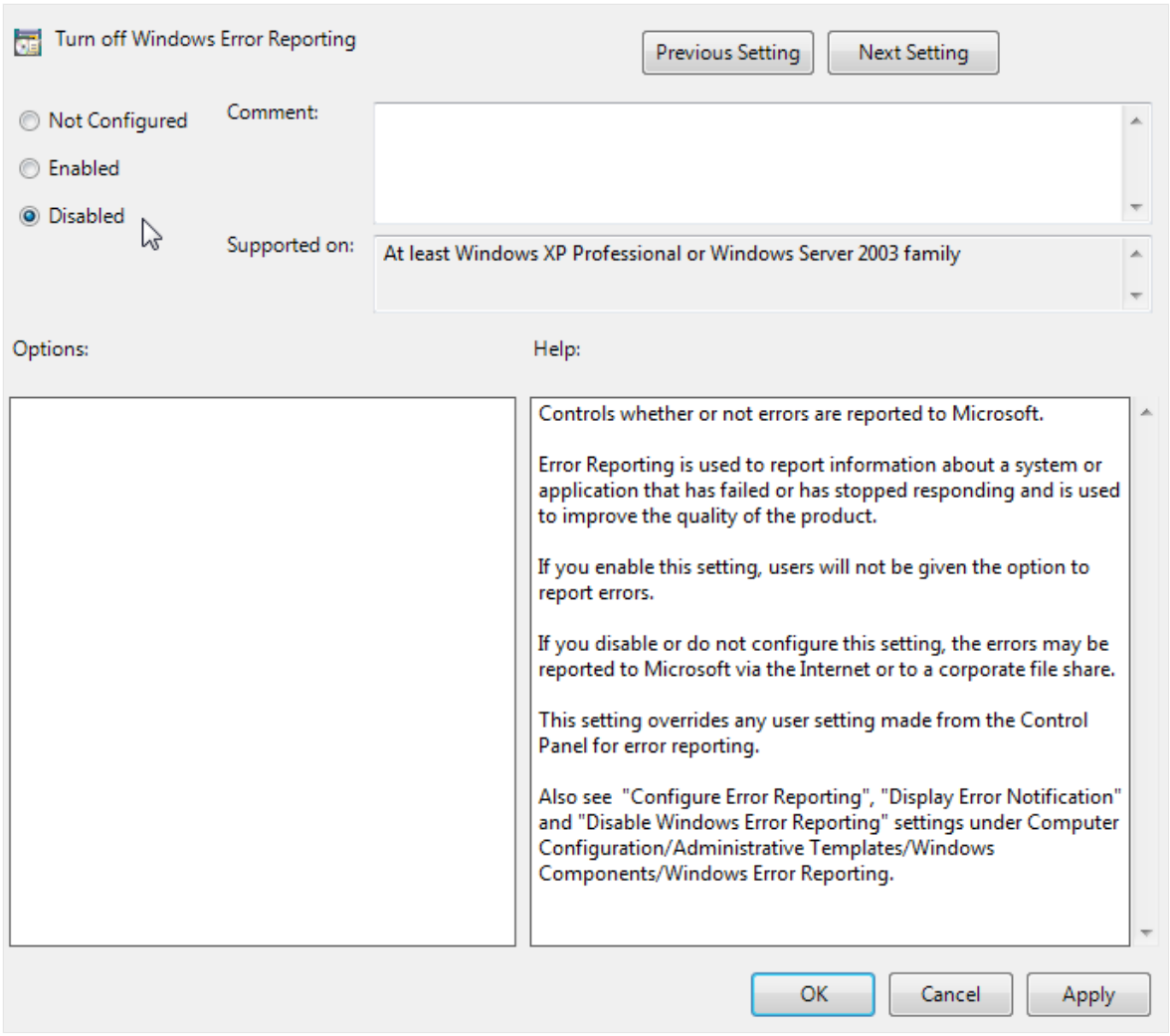
   > **Tip**
   >
   > Admins creating Group Policy Objects (GPOs) should be part of the Group Policy Creator Owners group in Active Directory (AD) or Domain/Enterprise Administrators.

2. Go to **Computer Configuration** > **Administrative Template** > **System** > **Internet Communication Management** > **Internet Communication Settings**.

3. Double-click the **Turn off Windows Error Reporting** policy.

4. Select **Disabled** > **Apply** > **OK**.



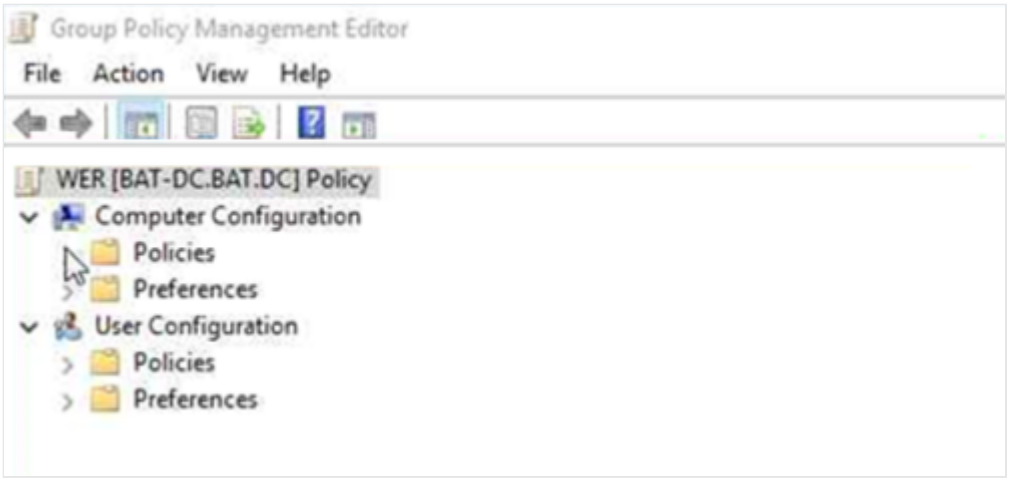
5. Go to **Computer Configuration** > **Administrative Template** > **Windows Components** > **Windows Error Reporting**.

6. Double-click the **Disable Windows Error Reporting** policy.

7. Select **Disabled** > **Apply** > **OK**.

Configure Windows diagnostic data (Telemetry)

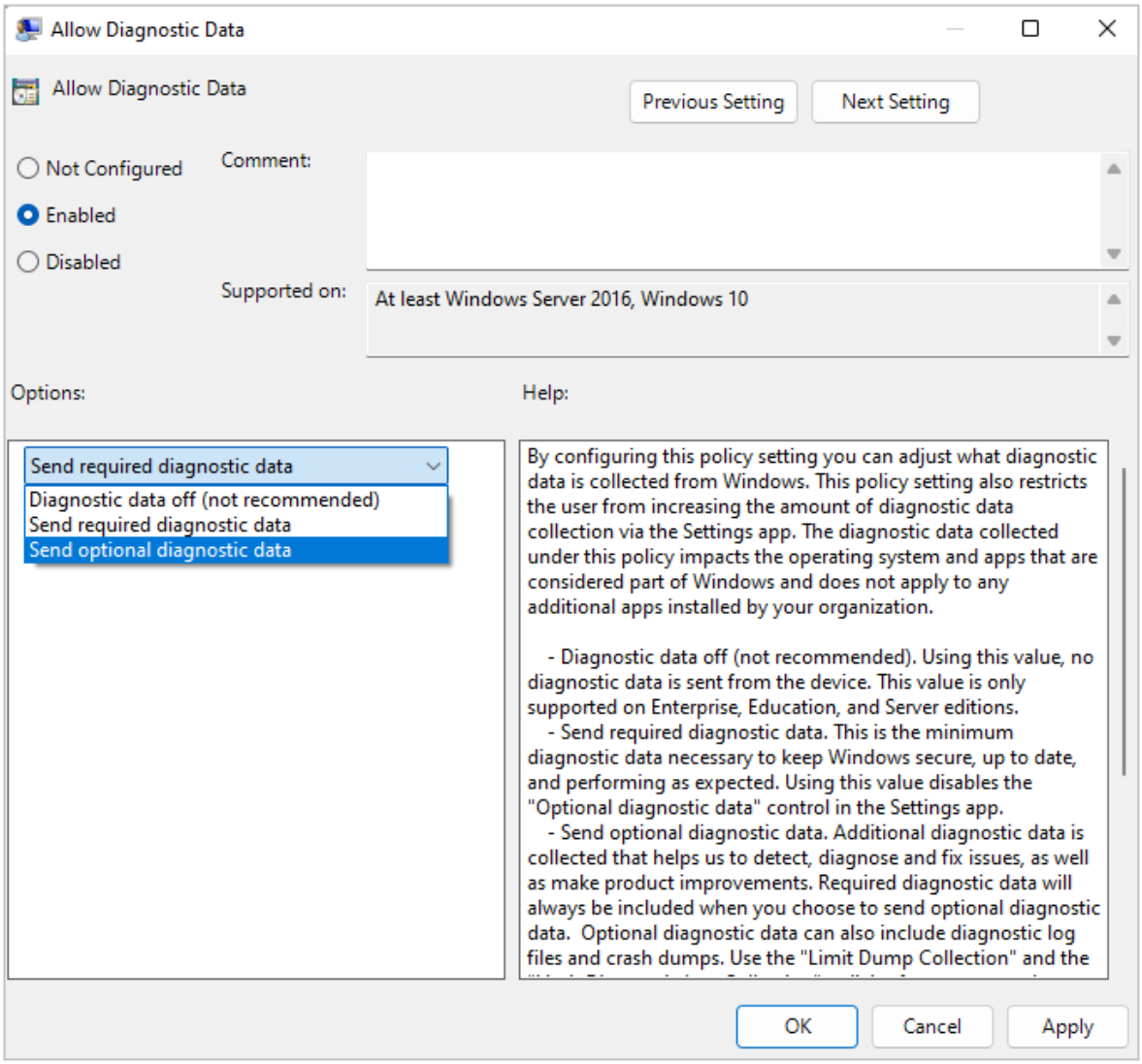
Expand **Policies** under **Computer Configuration** in **Group Policy Management Editor** (*gpmc.msc*).



Perform the following steps depending on the OS version:

For Windows 11

1. Go to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Data Collection and Preview Builds**.
2. Double-click the **Allow Diagnostic Data** policy.
3. Select **Enabled**, and then select the **Send optional diagnostic data** option from the **Options** drop-down list.

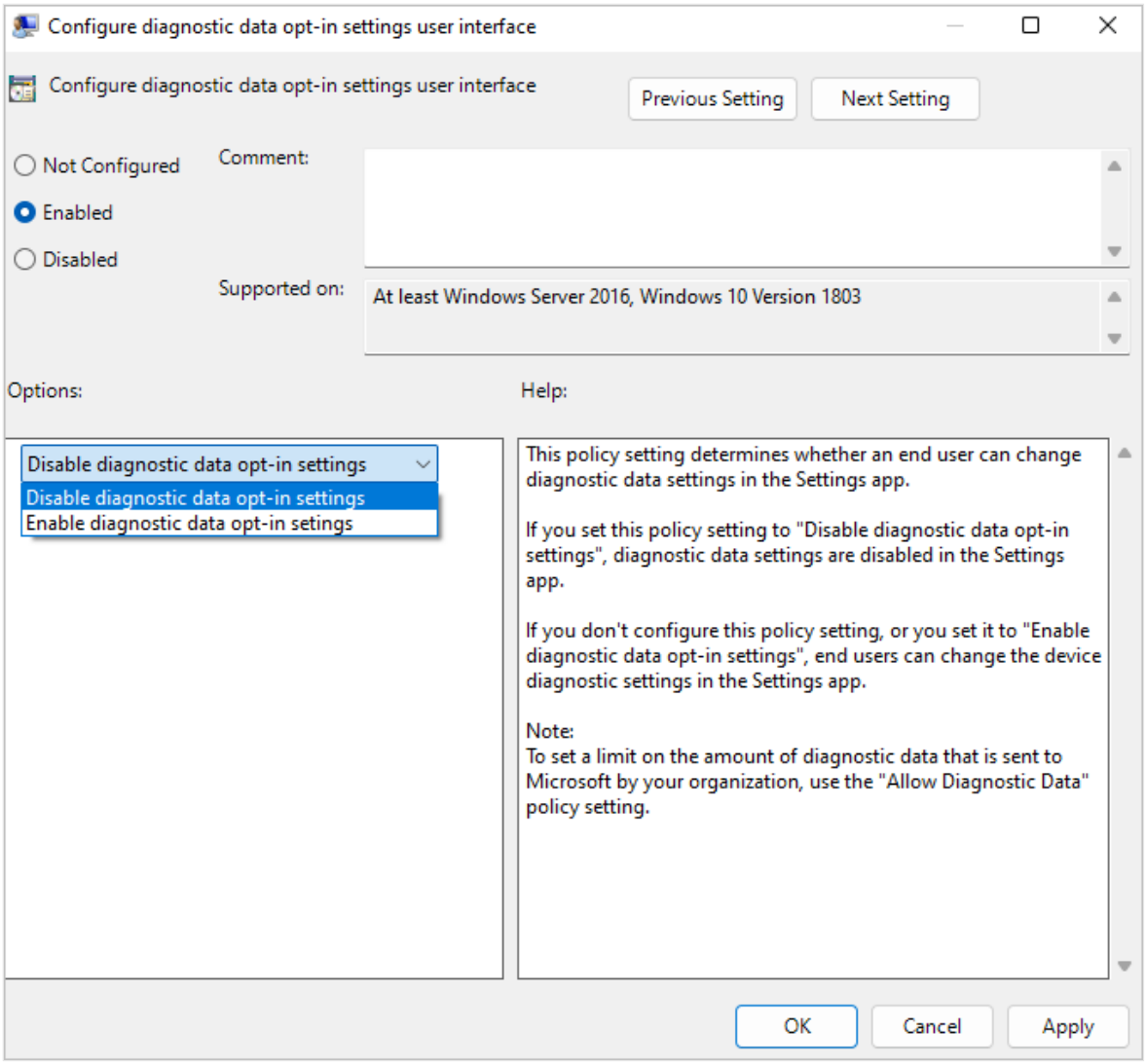


For more information about the level of data sent, see Diagnostics, feedback, and privacy in Windows.

4. Select **Apply** > **OK**.

5. Double-click the **Configure diagnostic data opt-in settings user interface** policy.

6. Select **Enabled**, and then select the **Disable diagnostic data opt-in settings** option from the **Options** drop-down list.

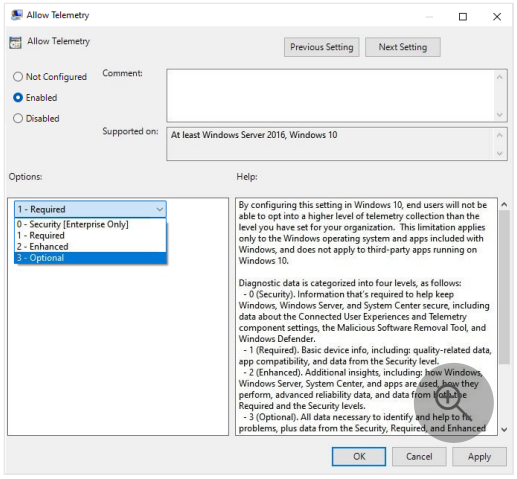
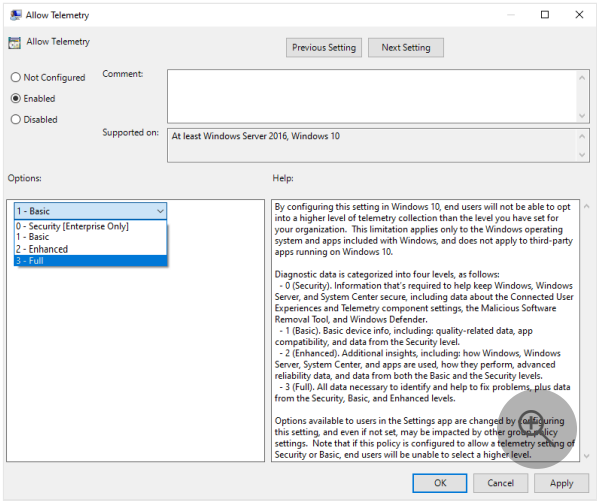


7. Select **Apply** > **OK**.

For Windows 10

1. Go to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Data Collection and Preview Builds**.
2. Double-click the **Allow Telemetry** policy.
3. Select **Enabled**.
4. From the **Options** drop-down list, select:
   - **Optional** for Windows 10, version 1903 or later
   - **Full** for Windows 10, version 1809 or earlier

Windows 10, version 1903 or later	**Windows 10, version 1809 or earlier**

Windows 10, version 1903 or later	Windows 10, version 1809 or earlier
	

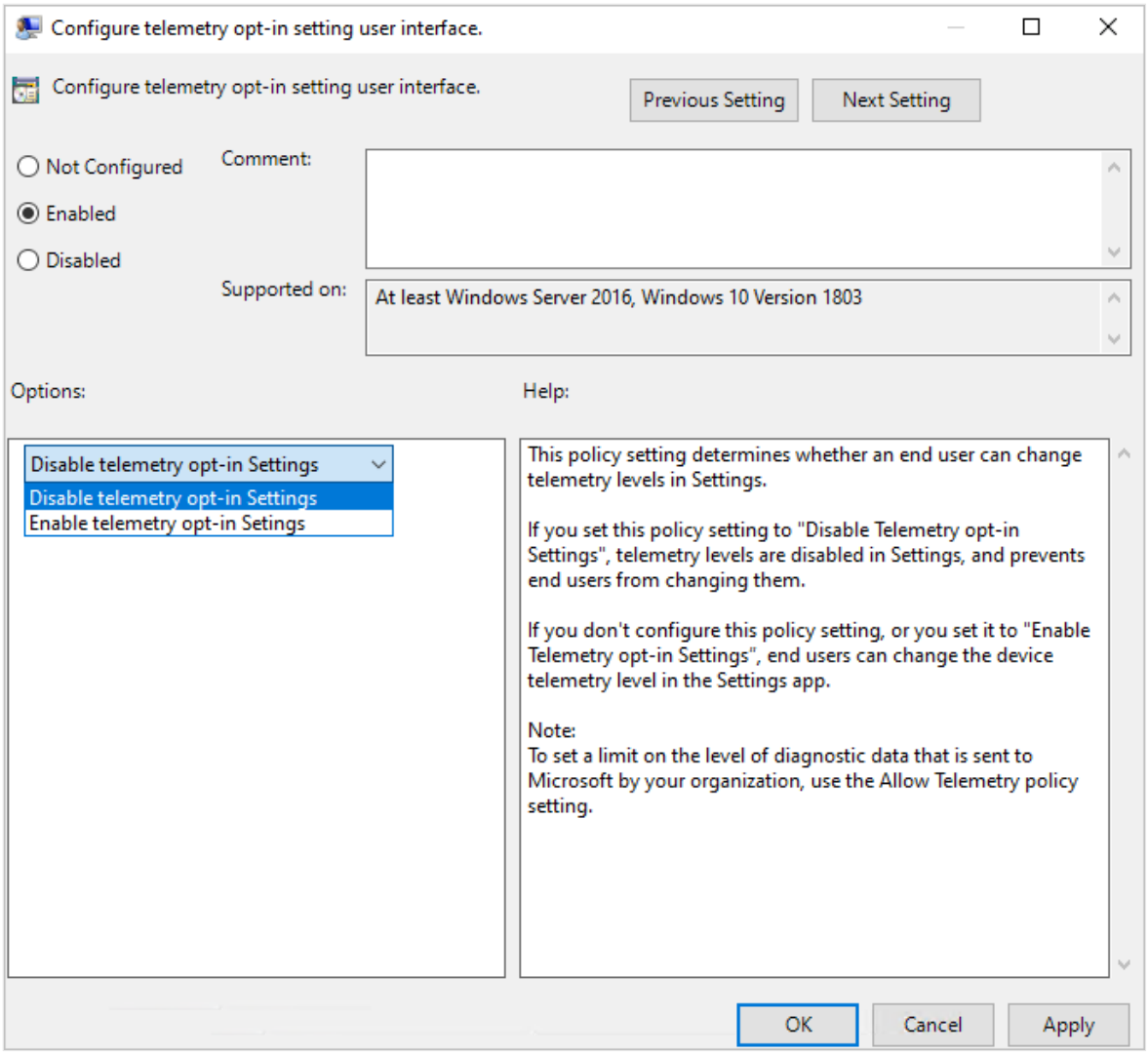
> **Note**
>
> Select at least the **Enhanced** option so that we can have enough actionable insights for Windows 10, version 1903 or later. For more information about the level of data collected, see **Diagnostic data settings**.

5. Select **Apply** > **OK**.

   The following steps require at least Windows 10, version 1803.

6. Double-click the **Configure telemetry opt-in setting user interface** policy.

7. Select **Enabled**, and then select the **Disable telemetry opt-in Settings** option from the **Options** drop-down list.



8. Select **Apply** > **OK**.

Configure network endpoints to be allowed

The following table lists the network endpoints related to how you can manage the collection and control of diagnostic data.

- Port used: 443
- Protocol used: HTTPS with SSL/TLS using certificate pinning

Windows versions	**Endpoint**
All Windows versions	watson.microsoft.com
Windows 10, version 1803 or later	watson.telemetry.microsoft.com
Windows 10, version 1809 or later	umwatsonc.events.data.microsoft.com
Windows 10, version 1809 or later	ceuswatcab01.blob.core.windows.net
Windows 10, version 1809 or later	ceuswatcab02.blob.core.windows.net

Windows versions	Endpoint
Windows 10, version 1809 or later	eaus2watcab01.blob.core.windows.net
Windows 10, version 1809 or later	eaus2watcab02.blob.core.windows.net
Windows 10, version 1809 or later	weus2watcab01.blob.core.windows.net
Windows 10, version 1809 or later	weus2watcab02.blob.core.windows.net

For more information, see Configure Windows diagnostic data.

Limit additional data from being sent to Microsoft (Optional)

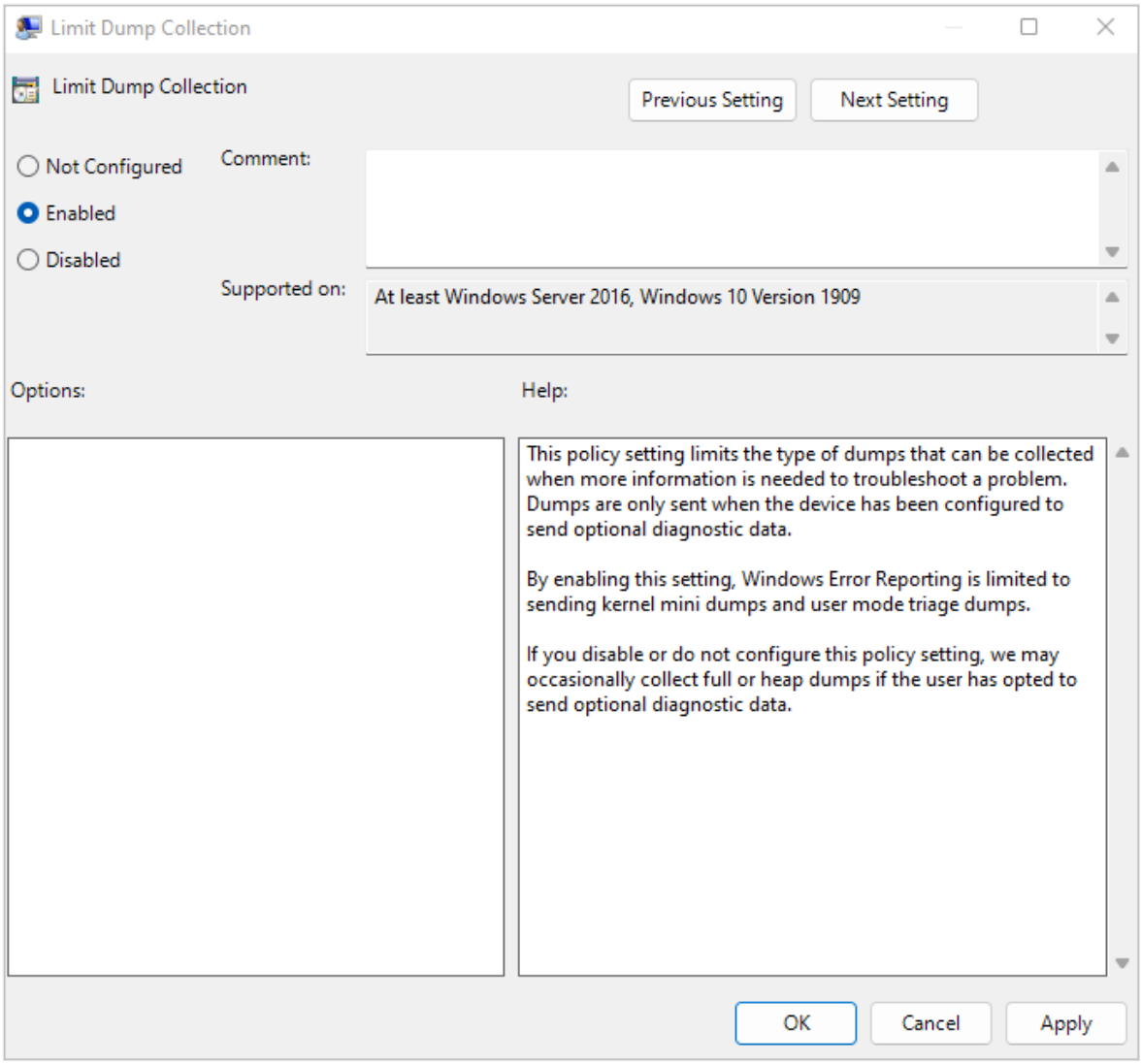
If the policies described in the article are enabled, Windows Error Reporting will send only kernel mini dumps and user mode triage dumps.

If you enable **Optional** data through Telemetry and want to control the type of dump information shared with Microsoft, you can use the following policies. These policies allow you to limit the types of crash dumps.

For Windows 11 and Windows 10 (version 1909 and later):

1. Go to **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Data Collection and Preview Builds**.

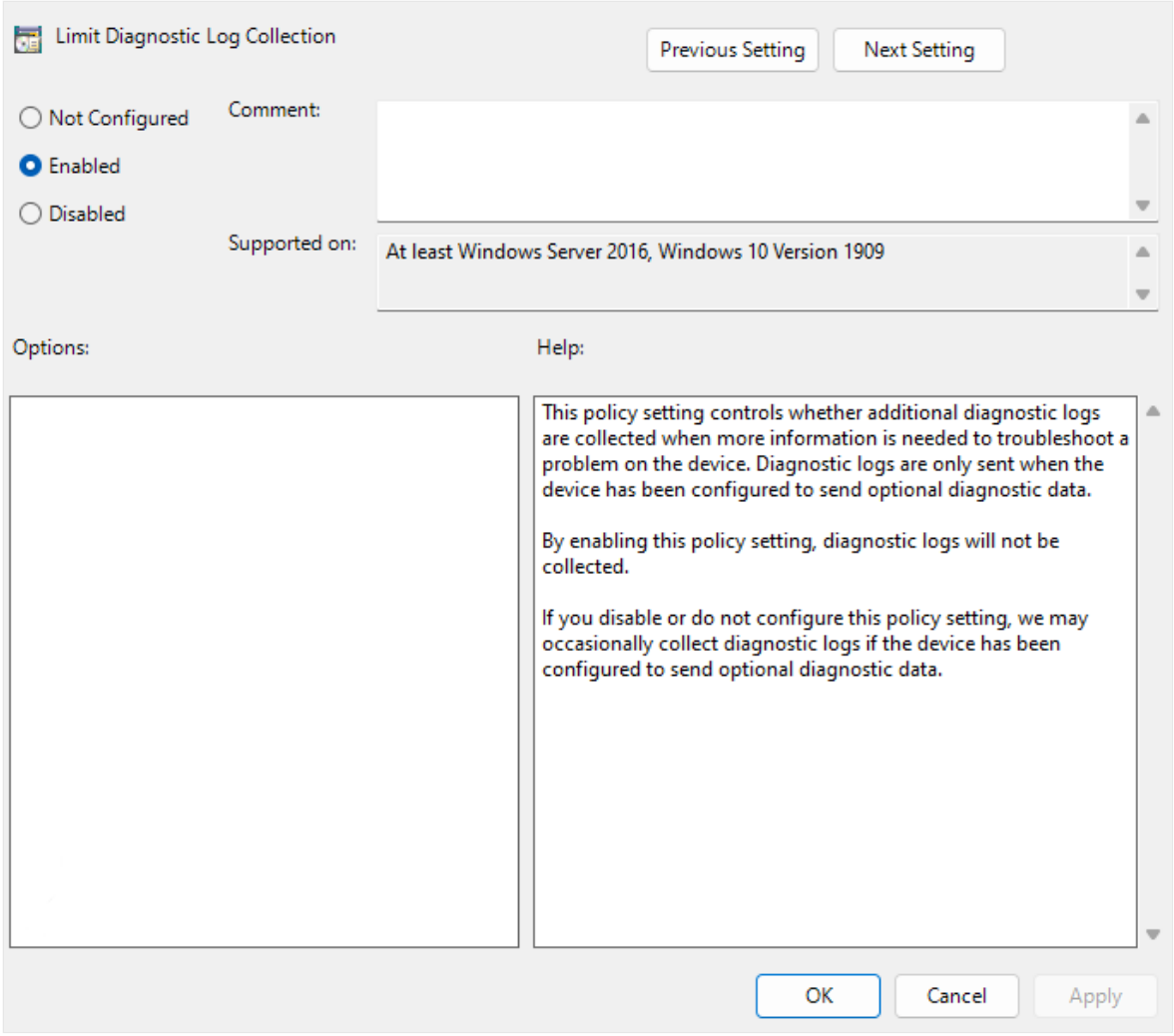
2. Double-click the **Limit Dump Collection** policy.



3. Select **Enabled** > **Apply** >**OK**.

4. Double-click the **Limit Diagnostic Log Collection** policy.

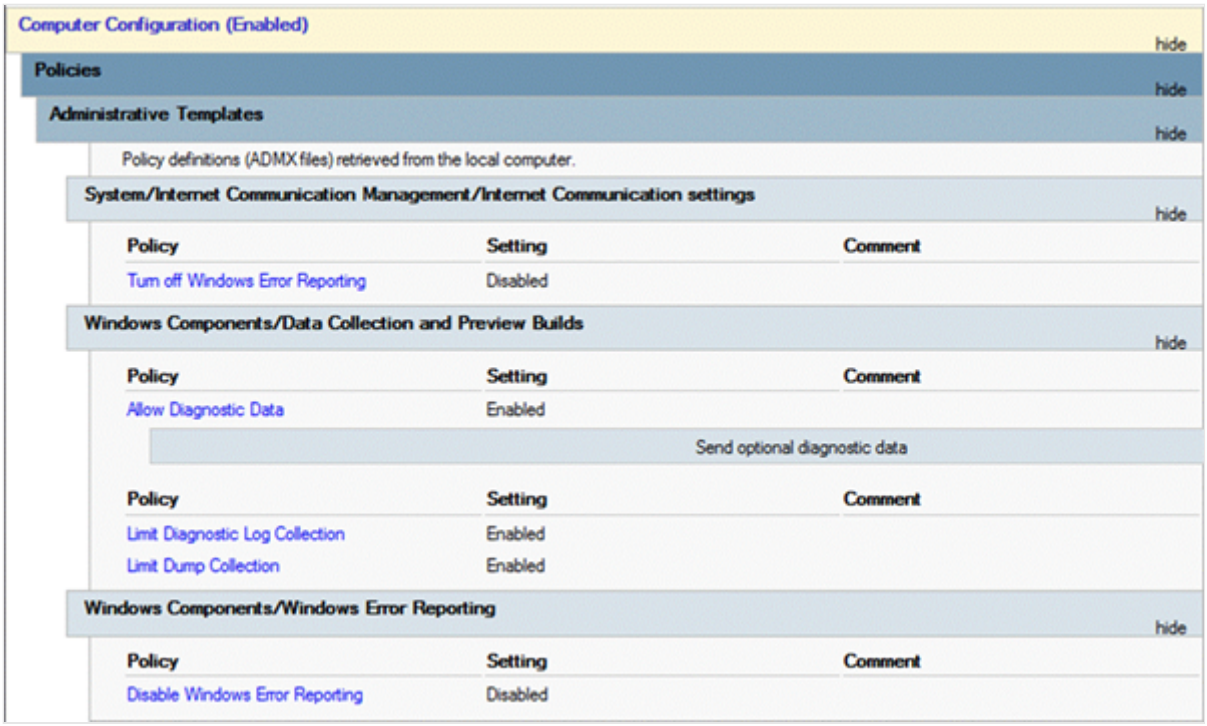
5. Select **Enabled** > **Apply** > **OK**.



For more information, see Configure types of dump to be collected.

Validate the correct data setting checklist

Your group policy object will have the following settings configured:



After you've applied the above-mentioned settings to the Organizational Unit, check the following items by using Registry Editor (*Regedit.exe*), and ensure the settings are configured and applied as desired on one of the machines:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection`

Registry Key Name	Data
`AllowTelemetry`	0x00000003
`DisableTelemetryOptInSettingsUx`	0x00000001
`LimitDiagnosticLogCollection`	0x00000001
`LimitDumpCollection`	0x00000001

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting`
  - **Registry Key Name**: `DoReport`
  - **Data**: 0x00000001

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting`

Registry Key Name	Data
`Disabled`	0x00000000
`DontSendAdditionalData`	0x00000001

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\Consent`
  - **Registry Key Name**: `DefaultConsent`
  - **Data**: 0x00000004

Gather key information before contacting Microsoft support

1. Download TSSv2 on all nodes and unzip it in the *C:\tss_tool* folder.
2. Open the *C:\tss_tool* folder from an elevated PowerShell command prompt.
3. Start the following traces on the problem computer by using the following cmdlets:

   ```PowerShell
   TSSv2.ps1 -SDP PERF,SETUP
   ```

   ```PowerShell
   TSSv2.ps1 -Start -Scenario NET_WFP
   ```

4. Respond to the EULA prompt.
5. Wait until the automated scripts finish collecting the required data.

The traces will be stored in a zip file in the *C:\MS_DATA\SDP_PERFSETUP* folder, which can be uploaded to the Microsoft workspace for analysis.

Errors when you run WinRM commands to check local functionality in a Windows Server 2008 environment

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to errors that occur when you run WinRM commands to check local functionality in a Windows Server 2008 environment.

Applies to: Windows Server 2012 R2
Original KB number: 2269634

Symptoms

When you run WinRM commands to check the local functionality on a server in a Windows Server 2008 environment, you may receive error messages that resemble the following ones:

> winrm e winrm/config/listener
> WSManFault Message = The client cannot connect to the destination specified in the requests. Verify that the service on the destination is running and is accepting request. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to analyze and configure the WinRM service: "winrm quickconfig"
> Error number:
> -2144108526 0x80338012

> winrm id
> WSMan Fault
> Message = The WinRM client received an HTTP bad request status (400), but the remote service did not include any other information about the cause of the failure.
> Error number:
> -2144108175 0x80338171

> winrm quickconfig
> WinRM is not set up to receive requests on this machine. The following changes must be made:
> Start the WinRM service.

> Make these changes [y/n]? y
> WinRM has been updated to receive requests.
> WinRM service started.

> WSManFault Message = The client cannot connect to the destination specified in the requests. Verify that the service on the destination is running and is accepting requests. Consult the logs and documentation for the WS-Management service running on the destination, most commonly IIS or WinRM. If the destination is the WinRM Service, run the following command on the destination to analyze and configure the WinRM Service: 'winrm quickconfig'.
> Error number: -2144108526 0x80338012

Cause

This problem may occur if the Window Remote Management service and its listener functionality are broken.

Resolution

To resolve this problem, follow these steps:

1. Install the latest Windows Remote Management update.
2. Run the following command to restore the listener configuration:

   ```
   Console
   winrm invoke Restore winrm/Config
   ```

3. Run the following command to perform a default configuration of the Windows Remote Management service and its listener:

   ```
   Console
   winrm quickconfig
   ```

How to configure WINRM for HTTPS

Article • 02/08/2022 • 2 minutes to read

This article provides a solution to configuring WINRM for HTTPS.

Applies to: Windows 10 - all editions
Original KB number: 2019527

Summary

By default WinRM uses Kerberos for authentication so Windows never sends the password to the system requesting validation. To get a list of your authentication settings, type the following command:

```
Console

winrm get winrm/config
```

The purpose of configuring WinRM for HTTPS is to encrypt the data being sent across the wire.

WinRM HTTPS requires a local computer Server Authentication certificate with a CN matching the hostname to be installed. The certificate mustn't be expired, revoked, or self-signed.

To install or view certificates for the local computer:

1. Select **Start** and then select **Run** (or using keyboard combination press Windows key+R)。
2. Type *MMC* and then press Enter.
3. Select **File** from menu options and then select **Add or Remove Snap-ins**.
4. Select **Certificates** and select **Add**.
5. Go through the wizard selecting **Computer account**.
6. Install or view the certificates under **Certificates (Local computer)** > **Personal** > **Certificates**.

If you don't have a Server Authenticating certificate, consult your certificate administrator. If you have a microsoft Certificate server, you may be able to request a certificate using the web certificate template from `HTTPS://<MyDomainCertificateServer>/certsrv`.

Once the certificate is installed type the following to configure WINRM to listen on HTTPS:

```
Console

winrm quickconfig -transport:https
```

If you don't have an appropriate certificate, you can run the following command with the authentication methods configured for WinRM. However, the data won't be encrypted.

```
Console

winrm quickconfig
```

More information

By default, on Windows 7 and later versions, WinRM HTTP uses port 5985 and WinRM HTTPS uses port 5986. On earlier versions of Windows, WinRM HTTP uses port 80 and WinRM HTTPS uses port 443.

To confirm WinRM is listening on HTTPS, type the following command:

```
Console

winrm enumerate winrm/config/listener
```

To confirm a computer certificate has been installed, use the Certificates MMC add-in or type the following command:

```
Console

Winrm get http://schemas.microsoft.com/wbem/wsman/1/config
```

If you get the following error message:

> Error number: -2144108267 0x80338115
> ProviderFault
> WSManFault
> Message = Cannot create a WinRM listener on HTTPS because this machine does not have an appropriate certificate.

To be used for SSL, a certificate must have a CN matching the hostname, be appropriate for Server Authentication, and not be expired, revoked, or self-signed.

Open the certificates MMC add-in and confirm the following attributes are correct:

- The date of the computer falls between the **Valid from:** to the **To:** date on the **General** tab.
- Host name matches the **Issued to:** on the **General** tab, or it matches one of the **Subject Alternative Name** exactly as displayed on the **Details** tab.
- That the **Enhanced Key Usage** on the **Details** tab contains **Server authentication**.
- On the **Certification Path** tab that the **Current Status** is **This certificate is OK**.

If you have more than one local computer account server certificate installed, confirm the Certificate Thumbprint displayed by `Winrm enumerate winrm/config/listener` is the same Thumbprint on the **Details** tab of the certificate.

How to use registry entries to configure standalone WMI providers

Article • 05/05/2022 • 2 minutes to read

Applies to: Windows 11

Symptoms

You experience a quota overflow error in a Windows Management Instrumentation (WMI) shared provider host process (WMIPrvSE.exe).

Resolution

The typical resolution for a WMIPrvSE.exe quota overflow is to configure standalone WMI providers. This custom configuration doesn't require administrative permissions.

In the past, you had to manually configure the providers. However, this article discusses a way to script these changes.

Previous resolution: Manually configure providers

To configure standalone providers, you previously had to run the following manual steps by using a Windows PowerShell script or command prompt:

1. Stop the existing suspect WMIPrvSE.exe process to clean the memory that's set in the proportional set size (PSS). To do this, run the following command:

   ```
   PowerShell
   kill -f <pid of suspect wmiprvse.exe process>
   ```

   > **Note**
   >
   > In this command, *<pid of suspect wmiprvse process>* represents the process ID (PID) of the Wmiprvse.exe process that generated the issue.

2. Use the `OWN` HostingmodelGroup to move the target working provider away from the suspect provider host. (Typically, this is a WMIPrvSE.exe share that's set as `HostingModel='NetworkserviceHost'`.) To do this, run the following command:

```PowerShell
$prv = gcim -namespace root/standardcimv2 __win32provider -filter
"name=<providername>"
$prv.HostingModel = $Prv.HostingModel + ":OWN"
```

> **Note**
>
> In this command, *<providername>* represents the name of the target working provider.

3. To set the new name, run the following command:

```PowerShell
set-ciminstance -inputobject $prv
```

New resolution

The new method for resolving this issue resembles the method that's discussed in Registry Keys and Values for Controlling Provider Security: Secure and compatible modes. This method involves creating a new registry subkey that contains entries that represent a list of the providers that require standalone hosting.

> **Important**
>
> If you have configured the provider security registry entries to run in secure or compatible mode, Windows ignores the **StandaloneProvider** entries.

The registry information uses the following structure:

- Subkey: **HKLM:\SOFTWARE\Microsoft\Wbem\CIMOM\StandaloneProviders**
- Entries (one per provider):
  - Name: ***Namespace*:*__TargetRelPath***

> **Note**
>
> In this string, *Namespace* represents the namespace of the target provider and *TargetRelPath* represents the relative path of the target provider. For example, **root\cimv2:__win32provider.name="MyProvider"**.

- Value: ***Integer***

> **Note**
>
> In this string, *Integer* represents a unique numeric index that identifies the provider.

You can use Registry Editor to manually configure the registry, or you can use a PowerShell script.

The following example script configures the registry information for the **StorageWMI** provider. In this example, index value for the provider is **50**.

PowerShell

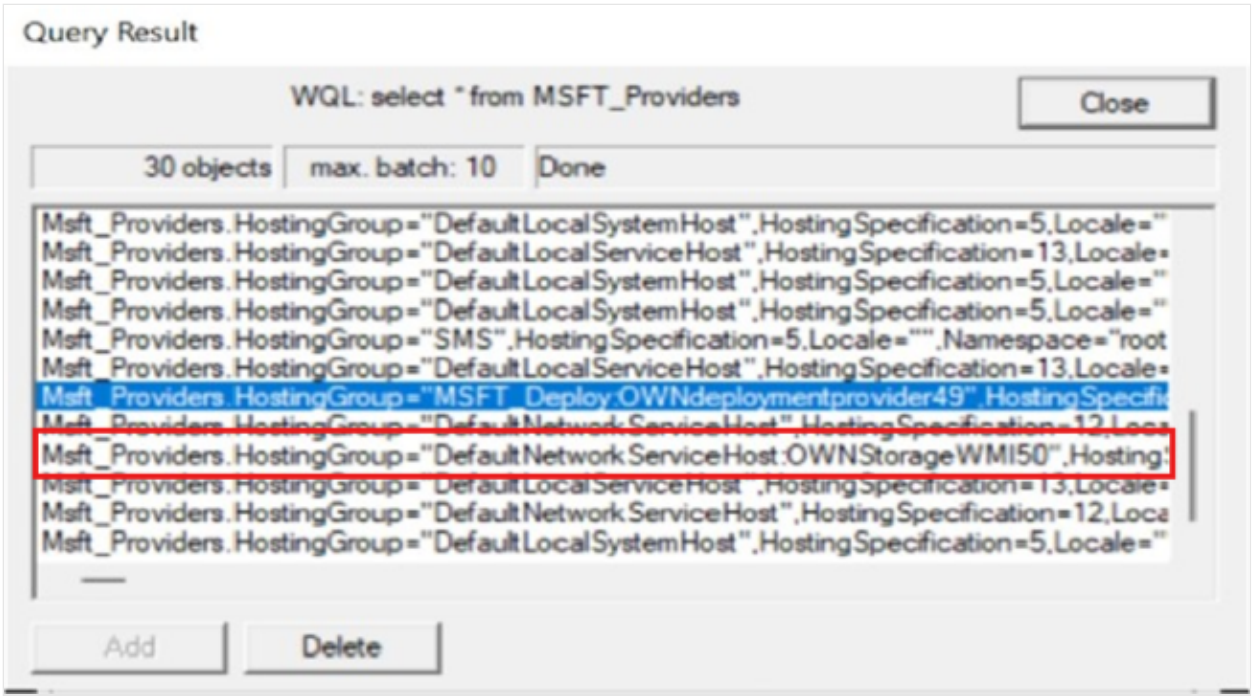
```
$registryPath = "HKLM:\SOFTWARE\Microsoft\Wbem\CIMOM\StandaloneProviders"
$Name = "ROOT/Microsoft/Windows/storage __win32provider.name='StorageWMI'"
$value = "50"
IF(!(Test-Path $registryPath))
  {
    New-Item -Path $registryPath -Force | Out-Null
    New-ItemProperty -Path $registryPath -Name $name -Value $value -
PropertyType String -Force | Out-Null
}
ELSE
{
    New-ItemProperty -Path $registryPath -Name $name -Value $value -
PropertyType String -Force | Out-Null
}
```

This script checks whether the subkey exists. If the subkey doesn't exist, the script creates it. Then, it creates the subordinate entry for **StorageWMI**. After the script makes this change, the provider runs in the standalone configuration, and the provider's hosting group information includes a string that resembles the following text:

Console

```
:OWNStorageWMI50
```

The following image shows how this listing appears in a list of providers.


Query Result
WQL: select * from MSFT_Providers
Close
30 objects
max. batch: 10
Done
Msft_Providers.HostingGroup="DefaultLocalSystemHost",HostingSpecification=5,Locale="
Msft_Providers.HostingGroup="DefaultLocalServiceHost",HostingSpecification=13,Locale=
Msft_Providers.HostingGroup="DefaultLocalSystemHost",HostingSpecification=5,Locale="
Msft_Providers.HostingGroup="DefaultLocalSystemHost",HostingSpecification=5,Locale="
Msft_Providers.HostingGroup="SMS",HostingSpecification=5,Locale="",Namespace="root
Msft_Providers.HostingGroup="DefaultLocalServiceHost",HostingSpecification=13,Locale=
Msft_Providers.HostingGroup="MSFT_Deploy:OWNdeploymentprovider49",HostingSpecifi
Msft_Providers.HostingGroup="DefaultNetworkServiceHost:OWNStorageWMI50",Hosting
Msft_Providers.HostingGroup="DefaultNetworkServiceHost",HostingSpecification=12,Loca
Msft_Providers.HostingGroup="DefaultLocalSystemHost",HostingSpecification=5,Locale="
Add
Delete

Event ID 10 is logged in the Application log

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution for the issue that Event ID 10 is logged in the Application log.

Applies to: Windows Server 2012 R2, Windows 10 - all editions
Original KB number: 950375

Symptoms

After you install Windows Vista Service Pack 1 (SP1) or Windows Server 2008, the following WMI error is logged in the Application log:

When you click the **Details** tab in the error message and then select the XML view, you receive the following error message:

> Event Xml:
> <Event xmlns="`http://schemas.microsoft.com/win/2004/08/events/event`"`>
> <System>
> <Provider Name="Microsoft-Windows-WMI" Guid="{1edeee53-0afe-4609-b846-d8c0b2075b1f}" EventSourceName="WinMgmt" />
> <EventID Qualifiers="49152">10</EventID>
> <Version>0</Version>
> <Level>2</Level>
> <Task>0</Task>
> <Opcode>0</Opcode>
> <Keywords>0x80000000000000</Keywords>
> <TimeCreated SystemTime="2008-01-18T22:37:27.000Z" />
> <EventRecordID>187</EventRecordID>
> <Correlation />
> <Execution ProcessID="0" ThreadID="0" />
> <Channel>Application</Channel>
> <Computer>adsd-PC</Computer>
> <Security />
> </System>
> <EventData>
> <Data>//./root/CIMV2</Data>

<Data>SELECT * FROM __InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA "Win32_Processor" AND TargetInstance.LoadPercentage > 99</Data>
<Data>0x80041003</Data>
</EventData>
</Event>

Cause

This problem occurs if the WMI filter is accessed without sufficient permission.

Resolution

To resolve this problem, run the script that is provided at the following Script Center website:

Event ID 10 is logged in the Application log on Windows Vista

This problem also occurs in Windows 7 and Windows Server 2008 R2. To resolve the problem in those systems, use the Fix it solution that is available in the following Microsoft Knowledge Base article:

2545227 Event ID 10 is logged in the Application log after you install Service Pack 1 for Windows 7 or Windows Server 2008 R2

More information

This particular Event ID 10 error message listed above can be safely ignored, it is not indicative of a problem with the Service Pack or with the operating system.

Failed logon event generated when running remote WMI command

Article • 09/23/2021 • 2 minutes to read

This article describes an issue where a failed logon event is generated when you run remote WMI command.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2816192

Symptoms

Consider the following scenario:

- You've two or more computers running Windows.
- The computers are set up in a workgroup or domain environment.
- You run a remote WMI query using an application that makes WMI calls from one computer to another computer.

In this scenario, if you review the Security log on the remote computer, you'll notice an Event ID 4625 that's for a failed logon with bad username or password. You'll also note then there's a successful logon with the credentials specified on the remote WMI query.

Cause

The pass-through authentication is always attempted first, even if specific credentials are specified in the tool being used.

Resolution

You can safely ignore the error message.

The SMS Agent Host service does not start after you restart a Systems Management Server 2003 client computer

Article • 09/23/2021 • 4 minutes to read

This article provides a resolution for the issue that SMS Agent Host service does not start after you restart a Systems Management Server 2003 client computer.

Applies to: Windows 10 - all editions
Original KB number: 922362

> **Important**
>
> This article contains information about how to modify the registry. Make sure to back up the registry before you modify it. Make sure that you know how to restore the registry if a problem occurs. For more information about how to back up, restore, and modify the registry, click the following article number to view the article in the Microsoft Knowledge Base:
> 256986 Description of the Microsoft Windows registry

Symptoms

After you restart a Microsoft Systems Management Server (SMS) 2003 client computer, the SMS Agent Host service (Ccmexec.exe) does not start. When this problem occurs, error entries that resemble the following ones may appear in the CCMExec.log file on the SMS client computer:

> CCMExec.log file entry 1
> Starting CCMEXEC service... $$<CcmExec><Fri Feb 13 8:13:13.819 2004 Central Standard Time><thread=1216 (0x4C0)>
> Running on machine **ComputerName** as user SYSTEM.
> $$<CcmExec><Fri Feb 13 8:13:13.859 2004 Central Standard Time><thread=1216 (0x4C0)>
> ERROR!! WBEM not found in the system path. $$<CcmExec><Fri Feb 13 8:13:13.859 2004 Central Standard Time><thread=1216 (0x4C0)>
> Successfully added WBEM to the process environment variable PATH. $$<CcmExec>

<Fri Feb 13 8:13:13.859 2004 Central Standard Time><thread=1216 (0x4C0)>
Initializing COM. $$<CcmExec><Fri Feb 13 8:13:13.859 2004 Central Standard Time><thread=1216 (0x4C0)>
Registering for logging change notifications. $$<CcmExec><Fri Feb 13 8:13:13.869 2004 Central Standard Time><thread=1216 (0x4C0)>
Setting default logging component for process. $$<CcmExec><Fri Feb 13 8:13:13.869 2004 Central Standard Time><thread=1216 (0x4C0)>
Setting service status to RUNNING. $$<CcmExec><Fri Feb 13 8:13:13.869 2004 Central Standard Time><thread=1216 (0x4C0)>
Checking if repair is required. $$<CcmExec><Fri Feb 13 8:13:13.889 2004 Central Standard Time><thread=1216 (0x4C0)>
Failed to open to WMI namespace '\\.\root\ccm' (80004002) $$<CcmExec><Fri Feb 13 8:13:17.224 2004 Central Standard Time><thread=1216 (0x4C0)>
CCMExec.log file entry 2
1/25/2006 9:16:35 PMFailed to open to WMI namespace '\\.\root\ccm' (8004100a)
1/25/2006 9:16:35 PMCCMDoCertificateMaintenance failed (0x8004100a).
1/25/2006 9:16:35 PMFailed to open to WMI namespace '\\.\root\CCM\Events' (8004100a)
1/25/2006 9:16:35 PMCCMDoCertificateMaintenance() raised CCM_ServiceHost_CertificateOperationsFailure status event.
1/25/2006 9:16:35 PMLoading service settings.
1/25/2006 9:16:35 PMFailed to open to WMI namespace '\\.\root\ccm\Policy\Machine' (8004100a)
1/25/2006 9:16:35 PMError loading service settings. Code 0x8004100a
1/25/2006 9:16:35 PMPhase 0 initialization failed (0x8004100a).
1/25/2006 9:16:35 PMService initialization failed (0x8004100a).
1/25/2006 9:16:35 PMShutting down AdditonallyCCMEXEC...
Additionally, the Wbemcore.log file may contain an error entry that resembles the following:
(Fri Feb 13 08:13:13 2004.69289) : Registry entry is indicating a setup is running
(Fri Feb 13 08:14:13 2004.129856) : CFactory construct
(Fri Feb 13 08:14:13 2004.129886) : CFactory destruct
(Fri Feb 13 08:14:13 2004.129896) : Created WINMGMT_ACTIVE mutex
(Fri Feb 13 08:14:13 2004.129946) : Reading config info from registry
(Fri Feb 13 08:14:16 2004.132800) : Preparing a namespace init request for active namespace //./ROOT/ccm/policy
(Fri Feb 13 08:14:16 2004.132901) : Preparing a namespace init request for active namespace //./root/CIMV2
(Fri Feb 13 08:14:16 2004.132961) : Preparing a namespace init request for active namespace //./root/subscription

> (Fri Feb 13 08:14:16 2004.133021) : Initializing namespace //./ROOT/ccm/policy
> (Fri Feb 13 08:14:16 2004.133041) : Initializing namespace //./root

Cause

This problem occurs when one or both of the following conditions are true:

- The %SystemRoot%\System32\Wbem path variable is not listed in the system path on the client computer.
- The type of the Path registry entry is incorrect on the SMS client computer.

The problem may also occur when the Windows Management Instrumentation (WMI) service does not start in a timely manner.

Resolution

To resolve this problem, use one of the following methods.

Method 1: Make sure that the %SystemRoot%\System32\Wbem variable is listed in the system path on the client computer

1. Click **Start**, click **Run**, type sysdm.cpl, and then click **OK**.
2. Click the **Advanced** tab, and then click **Environment Variables**.
3. Under **System variables**, click **Path**, and then click **Edit**.
4. Make sure that **%SystemRoot%\System32\Wbem** is listed in the **Variable value** box. If this value is not listed, you must add it. To do it, follow these steps:
   a. In the **Edit System Variable** dialog box, click after the end of text in the **Variable value** box, and then type:
   `;%SystemRoot%\System32\Wbem`
   b. Click **OK** three times to save the changes.

Method 2: Set the type of the Path registry entry to REG_EXPAND_SZ

> ⚠ **Warning**

> Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall your operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

1. Click **Start**, click **Run**, type regedit, and then click **OK**.
2. In Registry Editor, locate and then click the following registry subkey:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment`
3. Make sure that the type of the **Path** entry is REG_EXPAND_SZ and not REG_SZ. If the type of this entry is REG_SZ, you must copy the path information, delete the existing Path entry, and then create a new entry of type REG_EXPAND_SZ. To do it, follow these steps:
   a. In Registry Editor, double-click the **Path** value.
   b. Right-click the text in the **Value data** box, click **Copy**, and then click **Cancel**.
   c. Paste the text into a Notepad document.
   d. In Registry Editor, right-click **Path**, and then click **Delete**.
   e. On the menu bar, click **Edit**, point to **New**, and then click **Expandable String Value**.
   f. Type Path, and then press ENTER.
   g. Double-click **Path**.
   h. Right-click the **Value data** box, click **Paste**, and then click **OK**.
   i. Exit Registry Editor.

More information

For more information on troubleshooting Advanced Client Push Installations, see the following article in the Microsoft Knowledge Base:

928282 How to troubleshoot Advanced Client Push Installation Issues in Systems Management Server 2003 and System Center Configuration Manager 2007

WMI-Activity Event 5858 logged frequently with ResultCode 0x80041032

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution to solve the WMI-Activity event ID 5858 that's logged with ResultCode = 0x80041032 in Windows Server 2012 R2.

Applies to: Windows Server 2012 R2
Original KB number: 3124914

Symptoms

When using Windows Server 2012 R2 with applications that issue WMI queries using `IWbemServices:ExecQuery`, the administrator may observe the following event in Event Viewer:

Output

```
Log Name:  Microsoft-Windows-WMI-Activity/Operational
Source:    WMI-Activity
Event ID:  5858
Level:     Error
Id = {guid}; ClientMachine = <computer>; User = <user>; ClientProcessId =
<process ID>; Component = Unknown; Operation = Start
IWbemServices::ExecQuery - <WMI namespace>: <Select Query Statement>;
ResultCode = 0x80041032; PossibleCause = Unknown
where 0x80041032 indicates WBEM_E_CALL_CANCELLED.
```

> ⓘ **Note**
>
> This event can occur with many different ResultCode values. The problem described in this article only applies when `ResultCode = 0x80041032 (WBEM_E_CALL_CANCELLED)`.

Cause

WMI-Activity Error 5858 with ResultCode = 0x80041032 (WBEM_E_CALL_CANCELLED) indicates that the WMI caller has successfully issued `IWbemServices:ExecQuery`, but has released the `IWbemContext` object before retrieving the full result set using the `IEnumWbemClassObject::Next` method. If the WMI service is still holding data for the

client when the client terminates the link (by releasing the `IWbemContext` object), this event will be logged.

This error can happen if the WMI application calls `IEnumWbemClassObject::Next` with a timeout value (lTimeout) that is not long enough to retrieve the object being queried, and is not checking for a return code of `WBEM_S_TIMEDOUT (0x40004)` in order to issue the request again.

Resolution

The WMI client application should be modified to issue calls to `IEnumWbemClassObject::Next` to retrieve the full result set, before releasing the IWbemContext object. If no objects are received, make sure that the timeout value (lTimeout) is greater than **0** and that `WBEM_S_TIMEDOUT (0x40004)` is not being returned.

More information

For more information, see:

- IEnumWbemClassObject interface

  > **Note**
  >
  > The sample code included at the end of this page shows `IEnumWbemClassObject::Next` being called with a timeout value (lTimeout) of **0**, and is not checking for the **WBEM_S_TIMEDOUT** error.

- IWbemServices::ExecQuery method
- IEnumWbemClassObject::Next method

UE-V troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve UE-V-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

UE-V sub categories

- UEV 2.1
- User Experience Virtualization (UE-V)

%username% is unavailable in Windows that has OneDrive for Business installed

Article • 06/10/2022 • 2 minutes to read

This article provides a solution to an issue where %username% is unavailable in Windows that has OneDrive for Business installed.

Applies to: Windows 10 - all editions
Original KB number: 4551435

Symptoms

In a Windows installation that has OneDrive for Business installed, the **%username%** variable is intermittently unavailable. This causes applications that rely on this variable, such as User Experience Virtualization (UE-V), to work incorrectly.

Cause

In some cases, OneDrive for Business restarts the Windows Explorer process shortly after a user logs on. When this occurs, the **%username%** variable is not inherited by the new Explorer process. If you deployed UE-V by using the **%username%** variable as part of the "Settings Storage" setting, the literal string will be used. So all user accounts write to the same folder. This can cause high CPU activity on the server that hosts the network share.

Resolution

> ⚠ **Warning**
>
> Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

To fix this issue, enable one or both of the following registry keys to prevent OneDrive from restarting Explorer.

Per user OneDrive installation

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\OneDrive`

"HasSystrayIconBeenPromoted"=dword:00000001

Per computer OneDrive installation

- For 32-bit version of OneDrive:
  `HKEY_CURRENT_USER\SOFTWARE\Microsoft\OneDrive`
  "HasPerMachineSystrayIconBeenPromoted"=dword:00000001
- For 64-bit version of OneDrive:
  `HKEY_CURRENT_USER\SOFTWARE\Microsoft\OneDrive`
  "HasAMD64PerMachineSystrayIconBeenPromoted"=dword:00000001

Unexpected one-minute startup of Outlook if UE-V is enabled

Article • 09/23/2021 • 2 minutes to read

This article helps resolve an issue where you experience an unexpected one-minute delay for Outlook to start if UE-V is enabled in Windows 10, version 1809 or a later version of Windows.

Applies to: Windows 10 – all editions
Original KB number: 4569308

Symptoms

Consider the following scenario:

- You're using Outlook 2019 or Outlook 2016 on a computer that is running Windows 10, version 1809 or a later version of Windows.
- You install a cumulative update for Windows 10 that is released after March 17, 2020.
- You deploy User Experience Virtualization (UE-V) that has the **Sync Method** set to **None**.
- You register the MicrosoftOutlook2016CAWinXX.xml UE-V template. For example, you register MicrosoftOutlook2016CAWin32.xml.

In this scenario, Outlook takes one minute to start and display its splash screen.

Cause

This issue occurs when the **UE-V Sync** method is set to **None**. This setting causes Windows to ignore the synchronize timeout (by default, two seconds). Therefore, UE-V times out after one minute.

Resolution

To resolve this issue, use one of the following methods:

Method 1

Use the default Sync method **SyncProvider.**

The Sync method **None** is specific to workstations that have a permanent network connection to the **SettingsStoragePath**.

Method 2

Download and replace the version 3 of the Outlook custom action UEV template from the download center UE-V OutlookCA template update

More information

For more information, see the following articles:

- Unregister and register UE-V template
- Sync Methods for UE-V 2.x

How to enable debug logging in Microsoft User Experience Virtualization (UE-V)

Article • 09/23/2021 • 3 minutes to read

This article describes how to enable debug logging for the Microsoft User Experience Virtualization (UE-V) agent.

Applies to: Windows 10 - all editions
Original KB number: 2782997

Summary

It's useful when troubleshooting issues where settings or files aren't replicating as expected. Typically, this process is run on at least two different client machines to test replication.

More information

First, identify the scenario you wish to trace. The two main variations for UE-V are tracing applications and tracing desktop settings. User application traces can be collected when an executable is launched; desktop settings must be recorded during logoff and subsequent logoff.

Traces collect data for all users logged in to a computer. If you wish to record a trace for a non-administrator account, you will need to either log into a second desktop session (in the case of a Terminal Server, for example), or else launch a command prompt in the context of a member of the machine's local Administrators group by holding down the shift key and right-clicking on a shortcut to a Command Prompt. In addition, these commands must be run in an elevated token.

Scenario 1: Tracing an Application

1. Log on to the computer as a member of the local administrators group.
2. Launch an elevated command prompt by right-clicking on a shortcut to **Command Prompt** and selecting **Run as administrator**.

3. Create the trace definition by running these two commands in the elevated Command Prompt window:

```
Console

logman create trace UEV -P "Microsoft-User Experience Virtualization-
App Agent" -ow  -o uevtrace.etl
logman update UEV -P "Microsoft-User Experience Virtualization-Agent
Driver"
```

4. Start the trace by typing the command `logman start UEV`.
5. Close any running instances of the application you are investigating, then launch the application.
6. Reproduce the issue you are investigating, then close the application.
7. Stop the trace by typing `logman stop UEV`.
8. Delete the trace definition by typing `logman delete UEV`.
9. Decode the trace by typing the command `netsh trace convert uevtrace_000001.etl DUMP=TXT`.

> ⓘ **Note**
>
> The first trace you take will be named **uevtrace_000001.etl** by default. Edit the command above if you take multiple traces to reflect the name of the ETL file.

Scenario 2: Tracing a desktop settings issue

1. Log on to the computer as a member of the local administrators group.
2. Launch an elevated command prompt by right-clicking on a shortcut to **Command Prompt** and selecting **Run as administrator**.
3. Create the trace definition by running these two commands in the elevated Command Prompt window:

```
Console

logman create trace UEV -P "Microsoft-User Experience Virtualization-
App Agent" -ow  -o uevtrace.etl
logman update UEV -P "Microsoft-User Experience Virtualization-Agent
Driver"
```

4. Start the trace by typing the command `logman start UEV`.
5. Reproduce the issue you are investigating, then log off.
6. Log back on to the server.
7. Launch an elevated command prompt by right-clicking on a shortcut to **Command Prompt** and selecting **Run as administrator**.
8. Stop the trace by typing `logman stop UEV`.
9. Delete the trace definition by typing `logman delete UEV`.
10. Decode the trace by typing the command `netsh trace convert uevtrace_000001.etl DUMP=TXT`.

> ⓘ **Note**
>
> The first trace you take will be named **uevtrace_000001.etl** by default. Edit the command above if you take multiple traces to reflect the name of the ETL file.

Alternate method: Event Viewer logging

If you wish to use Event Viewer rather than text file logging, use the steps below.

1. Log on to the computer as a member of the local administrators group.
2. Launch **Event Viewer**.
3. Select **View\Show Analytic and Debug Logs.**
4. Navigate to **Event Viewer (Local)\Applications and Service Logs\Microsoft\User Experience Virtualization\App Agent**.
5. Right-click on **Debug** under **App Agent** and select **Enable Log**.
6. Select **OK** when presented with the "Analytic and Debug logs may lose events when they are enabled. Do you want to enable this log?" dialog.
7. Reproduce your issue.
8. Right-click **Debug** and select **Refresh**.
9. Right-click **Debug** and select **Disable Log**.

How to troubleshoot UE-V replication issues

Article • 09/23/2021 • 3 minutes to read

This article provides the steps to troubleshoot replication issues with Microsoft User Experience Virtualization (UE-V).

Applies to: Windows 10 - all editions
Original KB number: 2844022

Summary

Common scenarios include:

- Settings replicate from one machine to the Settings Storage Path but not from a second machine.
- Settings have replicated to the Settings Storage Path in the past, but are no longer either uploading or downloading correctly.
- Settings for some applications replicate, but not for other applications.

In general, it is recommended to test settings on at least two separate client computers and optionally two user accounts (computerA and computer, userA and userB in the example below). It is also recommended to investigate using a reference application such as Notepad for testing. Most commonly, issues will fall in to one of 4 broad scenarios:

- If settings replicate for UserA but not from UserB on the same computer, the problem lies with UserB.
- If settings replicate for neither UserA nor UserB on computerA, but do successfully replicate for both users on computerB, the problem is with computerA.
- If settings do not replicate for either user on either computer, the problem most likely resides in the server hosting the Settings Store Path, or in an infrastructure issue
- If settings replicate for UserA for some applications but not others, the problem most likely resides in the configuration of the problem application's template

Depending on the scenario, you are troubleshooting, use the steps below to further investigate the users, computers, or application templates experiencing the issue.

Isolate problem users, computers, or application templates

The checklist below provides a general framework for isolating problem users, computers, or application templates:

1. Examine the Microsoft-User Experience Virtualization-App Agent/Operational event log located under Event Viewer\Applications and Services Logs\Microsoft\User Experience Virtualization\App Agent. A successful synchronization will record an entry like the following:

   > Log Name: Microsoft-User Experience Virtualization-App Agent/Operational
   > Source: Microsoft-User Experience Virtualization-App Agent
   > Event ID: 2010
   > Task Category: Orchestrator
   > Description: User settings for the settings location template "Microsoft Notepad" have been successfully uploaded to the settings storage location.

2. Inspect the Microsoft-User Experience Virtualization-App Agent/Operational event log for any errors or warnings pertaining to the synchronization issue you are investigating.

3. Verify that location information is being updated as expected:

   a. Open a PowerShell window and navigate to the appropriate subfolder under %localappdata%\Microsoft\UEV%computername%. For each monitored template, there will be a folder that corresponds to the application's TemplateID (as reported by the `Get-UEVTemplate` command). Beneath this folder, the most current settings package file will be contained in a folder named *Current*.

   b. Check the date modified information (type `dir` in PowerShell and note the **LastWriteTime** column, or navigate to the folder in Explorer and reference the Date Modified setting). This should roughly correspond to the time of the last modification of the application.

   c. Compare the modified date of the file and the file size with the current package in the user's Settings Storage Path.(Get-UevConfiguration).settingsstoragepath data.

4. Run simultaneous traces on both machines to determine the point of failure. For more information, see How to enable debug logging in Microsoft User Experience Virtualization (UE-V).

5. If the UE-V synchronization method (`SynMethod`) is set to **OfflineFiles** (the default), verify that Client-Side Caching (also known as Offline Files) is enabled and working properly. See Managing Files and Folders for general information on how to implement and troubleshoot Client-Side Caching.

General troubleshooting notes

- Packages will only be modified if monitored settings are changed. In order to assess whether a package is being replicated, make one or more changes to the application's settings and wait for replication changes.
- Packages are replicated only when the application is launched or exited. Exceptions to this rule are desktop background, Ease of Access, and Desktop settings (Planning Which Applications to Synchronize with UE-V 1.0).
- Notepad is recommended as the preferred application for testing application data replication for UE-V because it is installed on all supported operating systems, is a relatively simple application, and familiar to most users. To test replication via Notepad, open Notepad.exe, click on **Format**, then click on **Font...**, modify the size of the font to the next available setting (that is, change **Size** from 11 to 12), then click **OK** to save settings. Exit Notepad to commit the changes. If necessary, repeat these steps on a second computer.

User Experience Virtualization (UE-V) registry settings

Article • 03/24/2022 • 5 minutes to read

This article describes UE-V registry settings.

Applies to: Windows 10 - all editions
Original KB number: 2770042

Summary

Settings defined via group policy will take precedence over settings defined in the locations of this table. Group policy-defined settings are stored at:

- `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\UEV\Agent\Configuration`
- `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\UEV\Agent\Configuration\Applications`
- `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\UEV\Agent\Configuration\WindowsSettings`
- `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\UEV\Agent\Configuration\CustomerExperienceImprovementProgram`
- `HKEY_LOCAL_MACHINE \Software\Policies\Microsoft\UEV\Management\CustomerExperienceImprovementProgram`
- `HKEY_CURRENT_USER\Software\Policies\Microsoft\UEV\Agent\Configuration`
- `HKEY_CURRENT_USER\Software\Policies\Microsoft\UEV\Agent\Configuration\Applications`
- `HKEY_CURRENT_USER\Software\Policies\Microsoft\UEV\Agent\Configuration\WindowsSettings`

Order of precedence for UE-V settings:

1. User-targeted settings managed by group policy. These configuration settings are stored in the registry key by group policy under:
   - `HKEY_CURRENT_USER\Software\Policies\Microsoft\Uev\Agent\Configuration`
   - `HKEY_CURRENT_USER\Software\Policies\Microsoft\Uev\Management`
2. Computer-targeted settings managed by group policy. These configuration settings are stored in the registry key by group policy under:

   `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Uev\Agent\Configuration`
3. Configuration settings defined by the current user using PowerShell or WMI. These configuration settings are stored by the UE-V agent under:

   `HKEY_CURRENT_USER\Software\Microsoft\Uev\Agent\Configuration`
4. Configuration settings defined for the computer using PowerShell or WMI. These configuration settings are stored by the UE-V agent under:

   `HKEY_LOCAL_MACHINE\Software\Microsoft\Uev\Agent\Configuration`

UE-V registry settings

The following table lists the registry settings that are used by the Microsoft User Experience Virtualization (UE-V) agent.

Setting Name	Setting Description	Registry Location	Registry Key Path	Registry Value name
Use User Experience Virtualization (UE-V)	Enables or disables User Experience Virtualization (UE-V) for applications and Windows settings.	`HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	SyncEnabled
Settings storage path	Configures where the user settings will be stored.	`HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	SettingsStoragePath
Settings template catalog path	Configures where custom settings location templates are stored.	`HKEY_LOCAL_MACHINE`	`\Software\Microsoft\UEV\Agent\Configuration`	SettingsTemplateCatalog

Setting Name	Setting Description	Registry Location	Registry Key Path	Registry Value name
Override Microsoft Templates	Configures whether the catalog is used to replace the default Microsoft templates installed with the UE-V agent. This setting is only applicable when a settings template catalog path is set.	`HKEY_LOCAL_MACHINE`	`\Software\Microsoft\UEV\Agent\Configuration`	OverrideMSTemplates
Specify the Synchronization Method	Configures whether the agent uses the Windows offline files feature to synchronize settings. None is available for computers that are always online and can tolerate not synchronizing during network outages.	`HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	SyncMethod
Enable Notification	Enables a notification message the import of application settings is delayed. This setting only applies with SyncMethod = None.	`HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	SettingsImportNotifyEnab
Notification Delay	The notification delay option specifies the delay before the notification appears. This setting only applies with SettingsImportNotifyEnabled = TRUE.	`HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	SettingsImportNotifyDela
Settings Package Prefetch	Specifies the application and Windows settings the UE-V agent pre-caches before the applications are launched. If Windows Settings are included in the prefetch list, the settings are available for future logins.	`HKEY_LOCAL_MACHINE`	`\Software\Microsoft\UEV\Agent\Configuration`	PrefetchPackageList
Synchronization timeout	Configures the number of milliseconds that the computer waits to retrieve settings before timeout.	`HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	SyncTimeoutInMillisecon
Package size warning threshold	Configures the UE-V agent to report when a settings package file size reaches a defined threshold.	`HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	MaxPackageFileSizeInByt
Offline Threshold	Defines the offline threshold in days after which the UE-V agent will not export settings when it comes back online. See More Information section for additional info on this setting.	`HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	OfflineThreshold
Preventing Overlapping Synchronization for Applications	Prevents the import of settings packages if an instance of the application is already open. This setting also prevents export at application shutdown if another instance of the application is open.	`HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	PreventOverlappingSynch

Setting Name	Setting Description	Registry Location	Registry Key Path	Registry Value name
Customer Experience Improvement Program	Specifies the setting for participation in the Customer Experience Improvement program. If set to true, then installer information is uploaded to the Microsoft Customer Experience improvement site. If set to false, then no information is uploaded	`HKEY_LOCAL_MACHINE`	Agent: `HKEY_LOCAL_MACHINE\Software\Microsoft\UEV\Agent\Configuration` Generator: `HKEY_LOCAL_MACHINE\Software\Microsoft\UEV\Management`	CustomerExperienceImpr
Hide Settings Package directory	Sets the visibility of the SettingsPackages folder created on the settings storage location. By default the folder is hidden and System. This setting must be defined before the folders are created.	`HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	HideSettingsPackagesFol
Roaming Windows settings	Configures the roaming of Windows settings.	`HKEY_LOCAL_MACHINE`	`\Software\Microsoft\UEV\Agent\Configuration\WindowsSettings`	ID of the settings locatior
Roaming Application settings	Configures the roaming of user settings of applications.	`HKEY_LOCAL_MACHINE`	`\Software\Microsoft\UEV\Agent\Configuration\Applications`	ID of the settings locatior
Active Directory Settings Storage Path	Records the Active Directory Home Directory. This setting should not be manually edited.	`HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	ADSettingsStoragePath
Install Time Stamp	Records installation data. This setting should not be manually edited.	`HKEY_LOCAL_MACHINE`	`\Software\Microsoft\UEV\Agent\Configuration`	InstallTimestamp
Excluded FileTypes	Identifies file types that will be excluded from settings synchronization	`HKEY_LOCAL_MACHINE`	`\Software\Microsoft\UEV\Agent\Configuration`	ExcludedFileTypes
Logoff Sync timeout value	Configures the number of milliseconds that the computer waits to sync settings before timeout	`HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER`	`\Software\Microsoft\UEV\Agent\Configuration`	LogOffWaitInterval

More information

Offline Threshold registry setting

This registry setting allows you to modify the offline threshold for the UE-V agent. By default the UE-V agent has an offline threshold of 30 days. If the computer has been offline for 30 consecutive days the UE-V agent will not synchronize settings changes that were made while offline to the settings storage location when the computer comes back on to the network. Instead the UE-V agent will import updated settings packages from the settings storage location first and then return to default synchronization behavior.

UserProfiles and Logon troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve UserProfiles and Logon-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

UserProfiles and Logon sub categories

- Slow logon
- User Logon fails
- User profiles

Slow logon with a blank screen in Windows

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue that makes Windows logon slow, with a blank screen displayed during the delay.

Applies to: Windows 10 - all editions
Original KB number: 3161390

Summary

Remote Desktop and console users experience a slow logon with a blank screen before the desktop is rendered in Windows. Longer logon times directly correspond to the number of desktop shortcuts that are defined in the user's profile.

Symptoms

In this situation, you might notice that the logon times increase continually. A blank screen may be displayed during this delay period. You may also notice that Explorer.exe consumes excessive CPU resources.

Additionally, Procmon shows that affected computers are busy accessing the following registry key:
`HKEY_USERS\S-1-5-21-xxxxxxx\Software\Microsoft\Windows\CurrentVersion\UFH\SHC` (or `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\UFH\SHC`)

You may also notice frequent changes or additions to shortcuts on the desktop. This might occur if you use a logon script to update the desktop or in a Remote Desktop situation in which the cached profile is deleted. This makes all entries new on the next logon.

Workaround

To work around this issue, configure a logon script to delete the following registry key during logon: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\UFH\SHC`

You can also use Group Policy preferences to work around this issue.

Note

There's a known issue when you use this workaround. As soon as the script is in place, users will see entries on the Start menu marked as "new" even though there aren't any newly installed applications or items. It might be a good idea to share this information with users to prevent them from logging a call with the Service Desk about this.

Integrated Unblock screen not displayed when smart card PIN is blocked

Article • 11/22/2021 • 2 minutes to read

Applies to: Windows 10

Assume that the **Allow Integrated Unblock screen to be displayed at the time of logon** group policy is enabled in Windows 10. After several failed logon attempts because of an incorrect PIN, the smart card is blocked and you receive this error message:

> The smart card is blocked. Please contact your administrator for instructions on how to unblock your smart card.

In this scenario, the Integrated Unblock screen isn't displayed.

To fix this issue, use one of the following methods and then try again to sign in to Windows by using the blocked smart card.

- Restart the computer.
- Use another method to sign in to Windows (such as username and password).
- Use another account to sign in to Windows and then sign out.
- Use the blocked smart card to sign in to another computer.

Registry keys for smart card PIN caching options are no longer available in Windows 10

Article • 09/23/2021 • 2 minutes to read

This article describes the changes in Windows 10 regarding the registry keys for smart card PIN caching options.

Applies to: Windows 10 - all editions
Original KB number: 4516455

Symptoms

In Windows 10, you find that the following registry settings no longer work:

- `HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication\Allow`
- `HKEY_LOCAL_MACHINE\SOFTWARE\GSC\Policies\PIN\Authentication\Minutes`

> **Note**
>
> These settings are described in more detail in **KB 2589130**.

Status

This behavior is by design.

More information

Smart card PIN caching behavior depends on the minidriver of the smart card reader. The minidriver should implement the PIN_CACHE_POLICY policy. At the time of PIN operation, the behavior of Smart Card BaseCSP is based on the cache policy parameters that are passed to it by the smart card minidriver.

Smart card minidriver vendors can control this behavior in their respective Smart Card Cryptographic Service Provider (CSP) or Key Storage Provider (KSP) products.

For more information, see PIN_CACHE_POLICY_TYPE and PIN_CACHE_POLICY.

If the smart card implements a Personal Identity Verification (PIV) card, a third-party minidriver is not required. This is because the minidriver for PIV is included in Windows.

We have a fixed PIN caching policy for the default minidriver for a PIV card. This policy is defined as follows:

- If the container is the digital signature container (according to the PIV specification), we forcibly assign a no-pin-caching policy.
- For any other container, we forcibly assign the standard PIN policy (PIN caching is enabled).

The registry locations that are mentioned in the "Symptoms" section are relevant only to the third-party minidriver that's affected by the issue that's described in KB 2589130. These registry locations are not used for all PIV cards. The affected PIV minidriver was used in 2011. Therefore, these registry settings aren't provided by Microsoft.

Custom credential providers don't load when you first log on

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue where custom credential providers do not work when you first log on.

Applies to: Windows 10 - all editions
Original KB number: 4073719

Symptom

Consider the following scenario:

- You have a Windows 10-based computer that is not joined to a domain.
- Custom credential providers are installed on the computer.
- You log on to the computer for the first time after it starts.

In this scenario, the custom credential providers are not called.

Cause

This is by design. A Windows 10 update improves the **Use my sign in info to automatically finish setting up my device after an update** sign-in option. This feature is used for first logon. Therefore, custom credential providers do not take effects.

Workaround

> ⚠ **Warning**
>
> Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

To work around this issue, disable automatic system logon of the last user by setting the following registry key:

- Location: `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
- Value name: DisableAutomaticRestartSignOn
- Value type: dword
- Value data: 1

Event 1098: Error: 0xCAA5001C Token broker operation failed in Windows 10

Article • 03/24/2022 • 2 minutes to read

This article provides help to solve an 0xCAA5001C error that occurs when you access Microsoft Store for Business on a Windows 10-based computer.

Applies to: Windows 10, version 1903, Windows 10, version 1809, Windows 10, version 1709
Original KB number: 3196528

Symptoms

After you log on to a Windows 10-based computer, you try to access Microsoft Store for Business. However, Azure Active Directory authentication fails, and some events are logged in the Microsoft-Windows-AAD/Operational log.

In addition to Microsoft Store for Business, this issue may affect Enterprise State Roaming.

Cause

This issue occurs if there are missing permissions or ownership attributes on one or both of the following registry keys:

- `HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\PSR`
- `HKEY_USERS\S-1-5-21-299502267-1950408961-849522115-1818\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\PSR`

> **Note**
>
> Match the SID reported for the user in event ID 1098 to the path under HKEY_USERS. In this example, it is S-1-5-21-299502267-1950408961-849522115-1818.

Resolution

To resolve this issue, follow these steps:

1. Take ownership of the key if necessary (Owner = SYSTEM).
2. Fix the permissions on these registry keys by enabling inheritance (fixing one should fix both, unless multiple users log on to the same device):
   - `HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\PSR`
   - `HKEY_USERS\S-1-5-21-299502267-1950408961-849522115-1818\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.AAD.BrokerPlugin_cw5n1h2txyewy\PSR`

Type	Principal	Access	Inherited from	Applies to

Type	Principal	Access	Inherited from	Applies to
Allow	S-1-15-2-1910091885-1573563583-1104941280-2418270861-3411158377-2822700936-2990310272	Query Value	None	This key only
Allow	SYSTEM	Full Control	CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData	This key and subkeys
Allow	Domain User Account (`user@contoso.com`)	Full Control	CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData	This key and subkeys
Allow	Administrators (COMPUTER\Administrators)	Full Control	CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData	This key and subkeys
Allow	CREATOR OWNER	Full Control	CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData	Subkeys only

> ⓘ **Note**
>
> If you view the permissions of the ~\PSR registry key under HKEY_USERS{SID}, the **Inherited from** field shows inheritance from the HKEY_USERS{SID} path.

If this does not resolve the issue, consider running Process Monitor while performing the authentication method to look for ACCESS DENIED in other areas of the registry or file system that could be causing the authentication failure. If you discover any, add them to this article.

Facial recognition logon doesn't work after you apply a Group Policy setting in Windows 10

Article • 09/23/2021 • 2 minutes to read

This article describes an issue that prevents you from logging on by using facial recognition. This issue is caused by a conflicting Group Policy setting (using facial recognition to unlock the device continues to work with the conflicting policy setting).

Applies to: Windows 10 - all editions
Original KB number: 3169080

Introduction

Windows Hello is a feature in Windows 10 that lets users log on and unlock their devices by using a preconfigured PIN, a fingerprint (if the device supports it), and facial recognition (if the device supports it).

With Windows Hello, users can perform authentication by providing their unique biometric identifier when they access the device-specific Microsoft Passport credentials. The Windows Hello authenticator works with Microsoft Passport to authenticate and let users log on to the enterprise network. Authentication doesn't roam among devices, isn't shared with a server, and can't easily be extracted from a device. If multiple employees share a device, each employee will use his or her own biometric data on the device.

Symptoms

Assume that you set up PIN and Facial Recognition credentials on a supported device that's running Windows 10. The following Group Policy setting is configured:
Interactive logon: Do not display last user name: Enable

After startup or a restart, you cannot use facial recognition for domain logon even when the fingerprint, password, and PIN are working. You can use facial recognition only to unlock the device.

When this issue occurs, the computer tries to use the camera and prompts you with "Looking for you Making sure its you," and then with "Windows Hello requires your PIN."

Cause

The following Group Policy setting does not currently allow logon or sign-on through facial recognition:

Computer Configuration/Local Policies/Security Options

Interactive logon: Do not display last user name: Enable

By default, this Group Policy setting is disabled.

Resolution

To resolve this issue, change this setting to Disabled , or wait for the anniversary update of Windows 10.

More Information

When Windows 10 was released, the operating system supported three Hello types:

- PIN. Before you can use Windows Hello to enable biometrics on a device, you must create a PIN to use as your initial Hello gesture. After youve set a PIN, you can add biometric gestures if you want to. You can always use the PIN to release your credentials. Therefore, you can still unlock and use your device even if you cant use your preferred biometric gesture because of an injury or if the sensor is unavailable or not working correctly.
- Facial recognition. This type uses special cameras that recognize an image in infrared (IR) light, which allows them to reliably tell the difference between a photograph or scan and a living person. Several vendors provide external cameras that incorporate this technology, and major laptop manufacturers are incorporating it into their devices.
- Fingerprint recognition. This type uses a capacitive fingerprint sensor to scan your fingerprint. Fingerprint readers have been available for Windows-based computers for years, but the current generation of sensors is significantly more reliable and less error-prone. Most existing fingerprint readers (whether external or integrated into laptops or USB keyboards) work with Windows 10.

For more information, see the Microsoft Passport guide.

First logon fails with error: The universal unique identifier (UUID) type is not supported

Article • 12/06/2021 • 2 minutes to read

This article describes a situation in which a user receives a UUID error message at the first logon of a Windows 8 or Windows 8.1 image. This issue occurs when the image was deployed by using System Center 2012 Configuration Manager or System Center 2012 R2 Configuration Manager.

Applies to: Windows 10 - all editions
Original KB number: 2976660

Symptoms

Assume that you use System Center 2012 Configuration Manager or System Center 2012 R2 Configuration Manager to deploy a Windows 8 or Windows 8.1 image. When a user starts the system that has the image (physical or virtual) and tries to sign in for the first time, they receive the following error message:

> The Group Policy Client service failed the sign-in.
> The universal unique identifier (UUID) type is not supported.



This error message appears at first user logon after initial deployment of the image. However, in some scenarios, later user logons also result in the error message.

After the message is displayed and the user selects **OK**, the logon screen is displayed again.

Cause

Winlogon communicates with the Group Policy service (GPSVC) through an RPC call upon system startup for computer policy. And it communicates with user logon for user policy. System Center Configuration Manager installs a Client-Side Extension (CSE) in the Windows image, which is detected by the Group Policy service on first start. The Group policy service then isolates itself into a separate SVCHOST process. The service was originally running in a shared process with other services. Because RPC communications have already been established before the service isolation, `Winlogon` can no longer contact the Group Policy service. This situation results in the error message that's described in the Symptoms section.

On later restarts, GPSVC is appearing in a separate process from the beginning of the operating system session. So, the RPC runtime has no problem finding the correct server process instance.

Resolution

> **ⓘ Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

The following workarounds can be used to avoid the error message. Both workarounds involve modifying the image build-in System Center Configuration Manager instead of implementing them in the already deployed image.

Workaround 1

Add a restart to the end of the task sequence list for the image build. Modify the System Center Configuration Manager task sequence for the image by using SMSTSPostAction `shutdown /r /t 0` as the last task before completing the build.

Workaround 2

Separate the Group Policy service into a separate SVCHOST instance. Implement the following command in the System Center Configuration Manager task sequence to set the corresponding registry entry:

Console

```
cmd /c reg add "HKLM\SYSTEM\CurrentControlSet\Services\gpsvc" /v Type /t
REG_DWORD /d 0x10 /f
```

By default, GPSVC isolates itself when detecting a CSE. This workaround will force GPSVC to always start in an isolated SVCHOST instance, including the first start. It prevents the registration of the RPC communications in different SVCHOST processes, and lets `Winlogon` successfully connect to the correct process.

Holding Shift key while shutting down or logging off may not disable automatic logon

Article • 09/23/2021 • 2 minutes to read

This article helps resolve an issue where you can't disable automatic logon by holding the Shift key while shutting down or logging off from a computer.

Applies to: Windows 10 – all editions
Original KB number: 2840544

Symptoms

Consider the following scenario:

- You connect a USB keyboard to a computer that is running Windows.
- Automatic logon is enabled.

  > **Note**
  >
  > To enable automatic logon, set the AutoAdminLogon registry value to 1 by using Registry Editor. For more information, see the More information section at the end of this KB article.

- You log off from the computer to log on with a different user account, holding down the Shift key on the USB keyboard after logging off to override the automatic logon setting.

In this scenario, the Secure Attention Sequence (logon) dialog box doesn't appear.

Resolution

To resolve this issue, be sure to hold down the Shift key before choosing to log off or restart the system. Alternatively, you can try pressing the Shift key multiple times.

More information

For more information about how to enable automatic logon in Windows, click the following article number to view the article in the Microsoft Knowledge Base:

310584 How to enable automatic logon in Windows

How to track users logon/logoff

Article • 09/23/2021 • 2 minutes to read

This article describes how to track users logon/logoff.

Applies to: Windows Server 2003
Original KB number: 556015

This article was written by Yuval Sinay, Microsoft MVP.

Summary

The following article will help you to track users logon/logoff.

Tips

Option 1

1. Enable Auditing on the domain level by using Group Policy:

   Computer Configuration/Windows Settings/Security Settings/Local Policies/Audit Policy

   There are two types of auditing that address logging on, they are **Audit Logon Events** and **Audit Account Logon Events**.

   Audit "logon events" records logons on the PC(s) targeted by the policy and the results appear in the Security Log on that PC(s).

   Audit "Account Logon" Events tracks logons to the domain, and the results appear in the Security Log on domain controllers only.

2. Create a logon script on the required domain/OU/user account with the following content:

   ```
   echo %date%,%time%,%computername%,%username%,%sessionname%,%logonserver% >>
   ```

3. Create a logoff script on the required domain/OU/user account with the following content:

   ```
   echo %date%,%time%,%computername%,%username%,%sessionname%,%logonserver% >>
   ```

> ⓘ **Note**
>
> Please be aware that unauthorized users can change this scripts, due the requirement that the SHARENAME$ will be writeable by users.

Option 2

Use WMI/ADSI to query each domain controller for logon/logoff events.

Community Solutions Content Disclaimer

Microsoft corporation and/or its respective suppliers make no representations about the suitability, reliability, or accuracy of the information and related graphics contained herein. All such information and related graphics are provided "as is" without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information and related graphics, including all implied warranties and conditions of merchantability, fitness for a particular purpose, workmanlike effort, title and non-infringement. You specifically agree that in no event shall Microsoft and/or its suppliers be liable for any direct, indirect, punitive, incidental, special, consequential damages or any damages whatsoever including, without limitation, damages for loss of use, data or profits, arising out of or in any way connected with the use of or inability to use the information and related graphics contained herein, whether based on contract, tort, negligence, strict liability or otherwise, even if Microsoft or any of its suppliers has been advised of the possibility of damages.

Cached user logon fails when LSASRV event 45058 indicates FIFO deletion of cached credential

Article • 09/23/2021 • 2 minutes to read

This article fixes a logon failure that occurs when logging on to a domain-joined Windows Vista or Windows 7 computer using cached credentials.

Applies to: Windows 7 Service Pack 1
Original KB number: 2555663

Symptoms

1. Users receive the following error when logging on to a domain-joined Windows Vista or Windows 7 computer using cached credentials:

   > There are currently no logon servers available to service the logon request.

2. LsaSrv Event 45058, logged in the System event log of a domain-joined workstation, indicates that the operating system has deleted the cached credential for the user specified in the event:

   > Log Name: System
   > Source: LsaSrv
   > Date: <date> <time>
   > Event ID: 45058
   > Task Category: Logon Cache
   > Level: Information
   > Keywords: Classic
   > User: N/A
   > Computer: `computername.contoso.com`
   > Description:
   > A logon cache entry for user `USERNAME@CONTOSO.COM` was the oldest entry and was removed. The timestamp of this entry was MM/DD/YYYY HH:MM:SS.

Cause

The user logon error occurs when a user's cached credentials have been purged from the local computer by more recent domain user logons.

Windows Vista and Windows 7 operating systems cache credentials for a finite number of user accounts (assuming cached credentials haven't been disabled).

Once the cached logon quota has been reached, the operating system will purge the oldest cached credential from the local computer so that the credentials for the next unique domain user successfully authenticated by a domain controller may be cached. The logging of the LsaSrv 45058 event indicates that the cached logon quota has been reached, triggering the deletion of the oldest user credential cached on the local machine.

Resolution

1. Verify that cache credentials are allowed on the local computer.

   If the CachedLogonsCount registry value is 0, then the system will not cache domain user credentials. See the **More information** section below to determine the configurable range.

2. If the user's credentials have been deleted OR cached credentials are disabled, establish network connectivity and name resolution with one or more domain controllers that can authenticate the user account's domain logon (VPN, and so on), then successfully authenticate the user's logon.

   If cached logons are enabled, a successful logon will cache that user's credentials while purging the oldest cached credentials.

   If establishing domain connectivity over a software VPN, you'll likely have to establish the VPN from another local or cached domain user, persist that connection while logging off, then logging on or switching to the domain user account whose credentials you want to cache.

3. Evaluate increasing the cache logon quota with a domain administrator.

More information

By default, a Windows operating system will cache 10 domain user credentials locally. When the maximum number of credentials are cached and a new domain user logs on to the system, the oldest credential is purged from its slot to store the newest credential. This LsaSrv informational event simply records when this activity takes place.

Once the cached credential is removed, it doesn't imply the account cannot be authenticated by a domain controller and cached again.

The number of slots available to store credentials is controlled by:

- Registry path: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`
- Setting Name: CachedLogonsCount
- Data Type: REG_SZ
- Value: Default value = 10 decimal, max value = 50 decimal, minimum value = 1

Cached credentials can also be managed with group policy by configuring:

Group Policy Setting path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options.

Group Policy Setting: Interactive logon: Number of previous logons to cache (in case domain controller is not available)

The workstation the user needs access to must have physical connectivity with the domain and the user must authenticate with a domain controller to cache their credentials again.

Can't configure a PIN when Convenience PIN and Hello for Business policies are enabled

Article • 09/23/2021 • 3 minutes to read

This article provides a resolution to make sure you can configure a PIN when Convenience PIN and Hello for Business policies are enabled in Windows 10.

Applies to: Windows 10 - all editions
Original KB number: 3201940

Symptoms

Users who are running Windows 10 Version 1607 or later version of Windows 10 and who are joined to an Active Directory domain cannot create a convenience PIN. Whereas users who are running Windows 10 Version 1511 or earlier can do so without a problem.

When users navigate to **Settings** > **Accounts** > **Sign-in options**, the option to set a PIN is unavailable (appears dimmed), and therefore it can't be configured.

A user has already configured a convenience PIN in an earlier version of Windows 10, and then upgrades to Windows 10 Version 1607 or later. The PIN works until the user navigates to **Settings** > **Accounts** > **Sign-in options** > **I forgot my PIN**. In this situation, the option to create a PIN is unavailable (appears dimmed). This issue doesn't affect Windows 10 Version 1511 and earlier.

Cause

Windows 10 Version 1607 and later include new functionality that differentiates Windows Hello for Business from a convenience sign-in PIN.

Windows Hello for Business has strong user authentication properties that are frequently and mistakenly assumed to be functioning when the Windows Hello for Business infrastructure isn't in place and when a user is using a convenience PIN. This change prevents the creation of a PIN in Windows 10 and later version without Windows Hello for Business.

Additionally, a user can't create a convenience PIN in Windows 10 version 1607 and later version when the following policies are both enabled, unless the device is joined to

Azure Active Directory in some way:

- Use Convenience PIN
- Use Windows Hello for Business

For example, the device is either Azure AD-joined, or has the following policy enabled:

Computer Configuration\Administrative Templates\Windows Components\device registration\Register domain joined computers as devices

To allow convenience PINs to be created on devices that aren't joined to Azure AD, make sure that the following conditions are true:

- The Use Windows Hello for Business policy isn't enabled.
- The Turn on convenience PIN sign-in policy is enabled.

Resolution

To use a convenience PIN in Windows 10 Version 1607 or later, the following Group Policy setting must be configured:

- Policy: Turn on convenience PIN sign-in
- Category: Path Computer Configuration\Administrative Templates\System\Logon

> ⓘ **Note**
>
> - The GPO specifies Windows Server 2012, Windows 8, Windows RT, Windows Server 2012 R2, Windows 8.1, and Windows RT 8.1 only. This is incorrect and will be updated at a later date. This policy does apply to Windows 10 and lets the user set a convenience PIN.
> - Enabling a PIN in this manner doesn't provide the same level of security as using a PIN with the Windows Hello for Business infrastructure configured.

PIN complexity: Manage PIN complexity in the standard way by using policies that are found in the following location:

Computer Configuration\Administrative Templates\Windows Components\Windows Hello for Business \PIN Complexity

Don't configure settings other than PIN complexity if you want to use a convenience PIN. Having Windows Hello for Business and Turn on convenience PIN sign-in enabled prevents you from setting a PIN.

More information

When Windows Hello for Business isn't in place and a user has a convenience PIN configured, the user is using a password stuffer, which doesn't have any of the security qualities of Windows Hello for Business. Password stuffers are convenience sign-in PINs. They are controlled by the Turn on convenience PIN sign-in Group Policy setting.

Microsoft made this default behavior since Windows 10 Version 1607. The security offered by this default behavior can be decreased at the user's own discretion by enabling a convenience PIN.

For more information, see Windows Hello for Business.

Identify a damaged user profile and create a new profile in Windows Server 2003

Article • 09/23/2021 • 2 minutes to read

This article describes how to determine whether a user profile is damaged and how to create a new profile if the profile is damaged.

Applies to: Windows Server 2003
Original KB number: 816593

Summary

User profiles automatically create and maintain the desktop settings for each user's work environment on the local computer. A user profile is created for each user when the user logs on to a computer for the first time.

Identify a damaged profile

To determine whether a user account has a damaged user profile, follow these steps:

1. Create a new user account. Give it the same rights and group memberships or associations as the account that has the profile that you suspect may be damaged.

2. Copy the user settings in the suspect profile to the profile of the newly created user account. To do this, follow these steps:
   a. Click **Start**, point to **Control Panel**, and then click **System**.
   b. Click **Advanced**, and then under **User Profiles**, click **Settings**.
   c. Under **Profiles stored on this computer**, click the suspect user profile, and then click **Copy To**.
   d. In the **Copy To** dialog box, click **Browse**.
   e. Locate the **drive**:\Documents and Settings**user_profile** folder, where **drive** is the drive where Windows is installed, and where **user_profile** is the name of the newly created user profile, and then click **OK**.
   f. Click **OK**, click **Yes** to overwrite the folder contents, and then click **OK** two times.

3. Use the newly created user account to log on. If you experience the same errors that led you to question the suspect user profile, the user profile is damaged. If you do not experience any errors, it is the user account that is damaged.

Delete and re-create a profile

If the user profile is damaged, you must delete the profile, and then create a new profile for that user. To do this, follow these steps:

1. Use an administrator account to log on to the computer that contains the damaged user profile.
2. Open Control Panel, and then select **System**.
3. Click the **Advanced** tab, and in the **User Profiles** area, click **Settings**.
4. In the **Profiles stored on this computer** list, select the appropriate user profile, and then click **Delete**.
5. When you are prompted, click **Yes**.
6. Log off with the administrator account.
7. Use the account that had the damaged user profile to log on. A new user profile is created for the user.

Error "Invalid store path" during the LoadState process when you use the User State Migration Tool

Article • 09/23/2021 • 2 minutes to read

This article helps to fix the error "Invalid store path" during the LoadState process when you use the User State Migration Tool.

Applies to: Windows 10 - all editions
Original KB number: 2892374

Symptoms

Assume that you are using the User State Migration Tool (USMT) to migrate user profiles to Windows 8 or Windows 7. When you run the LoadState command on the destination computer, you receive the following error message:

> Invalid store path; check the store parameter and/or file system permissions

However, the path contains a valid migration store MIG file.

Cause

This issue occurs because the migration store path that is specified in the LoadState command points directly to the location of the MIG file. However, it must point to the root folder instead.

Resolution

To resolve this issue, provide a path of the same folder level that was used in the scan state. Do not use the full path in the command.

For example, if the MIG file is located at "C:\store\usmt\usmt.mig," the LoadState command should be pointed to "C:\store" as follows: Loadstate.exe c:\store /auto

More information

For more information, go to USMT 4.0: Cryptic messages with easy fixes .

Error (Roaming profile was not completely synchronized) and logon, logoff delays in Windows 10, version 1803

Article • 09/23/2021 • 2 minutes to read

This article provides help to fix errors, and logon/logoff delays that occur when you use roaming user profiles in Windows 10, version 1803.

Applies to: Windows 10, version 1803
Original KB number: 4340390

Symptoms

On a computer that's running Windows 10, version 1803, you experience logon or logoff delays when you use roaming user profiles. You also receive the following error messages:

> Your roaming profile was not completely synchronized. See the event log for details or contact administrator"

Additionally, the system may log the following entries in the event log.

- Event 1509 (source: User Profile General)

  Output

  ```
  Windows cannot copy file \\?
  \C:\Users\%username%\AppData\Local\Microsoft\Windows\<Path to a file>
  to location \\?\UNC Path\%username%.V6\AppData\Local\Microsoft\Windows\
  <path to a file>. This error may be caused by network problems or
  insufficient security rights.
  DETAIL - Access is denied.
  ```

- Event 509 (source: User Profile General)

  Output

  ```
  Windows cannot copy file \\?
  \C:\Users\UserName\AppData\Local\Microsoft\Windows\UPPS\UPPS.bin to
  location \\?\UNC
  ```

```
Path\UserName.V6\AppData\Local\Microsoft\Windows\UPPS\UPPS.bin. This
error may be caused by network problems or insufficient security
rights.
DETAIL - Access is denied.

Windows cannot copy file \\?
\C:\Users\UserName\AppData\Local\Microsoft\WindowsApps\Microsoft.Micros
oftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe to location \\?
\UNC\WS2016DC1\rup\UserName.V6\AppData\Local\Microsoft\WindowsApps\Micr
osoft.MicrosoftEdge_8wekyb3d8bbwe\MicrosoftEdge.exe. This error may be
caused by network problems or insufficient security rights.
DETAIL - The file cannot be accessed by the system.

Windows cannot copy file \\?
\C:\Users\UserName\AppData\Local\Microsoft\WindowsApps\MicrosoftEdge.ex
e to location \\?
\UNC\WS2016DC1\rup\UserName.V6\AppData\Local\Microsoft\WindowsApps\Micr
osoftEdge.exe. This error may be caused by network problems or
insufficient security rights.
DETAIL - The file cannot be accessed by the system.
```

- Event 1504 (source: User Profile General)

Output

```
Windows cannot update your roaming profile completely. Check previous
events for more details.
```

Cause

This problem occurs because of a change that was made in Windows 10, version 1803. This change inadvertently caused folders that are usually excluded from roaming to be synchronized by roaming user profiles when you log on or log off.

Resolution

This problem is fixed in the following update for Windows 10, version 1803:

July 24, 2018-KB4340917 (OS Build 17134.191)

Workaround

Important

> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

To work around this problem, you can copy the ExcludeProfileDirs registry key from a Windows 10, version 1709-based computer to the version 1803-based computers that are experiencing the problem. Full path to the registry key:

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\ExcludeProfileDirs`

For information about how to export and import registry keys by using the reg.exe tool, see the following Windows IT Pro Center article:

reg export

Renaming a user account doesn't automatically change the profile path

Article • 09/03/2022 • 2 minutes to read

When you rename a user account on a computer that is running Windows 7 or Windows Server 2008 R2, the user profile path isn't changed automatically. It may cause some confusion when the `%SystemDrive%\users` folder is viewed. This article provides a workaround for this issue.

> **Important**
>
> Don't apply the workaround to computers that are running Windows 10 or later. It can cause the `winget` command to stop working.

Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
Original KB number: 2454362

Status

Microsoft has confirmed it to be by design in Windows.

Workaround

To work around this issue, use the steps below to manually rename the profile path.

1. Log in by using another administrative account.

   > **Note**
   >
   > You may need create a new administrative account at first.

2. Go to the `C:\users\` folder and rename the sub folder with the original user name to the new user name.

3. Go to registry and modify the registry value **ProfileImagePath** to the new path name.

   > **Important**

> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\<User SID>\`

> **Note**
>
> Replace <User SID> with the SID of your user account.

4. Log out and log in again by using the user whose name is changed, and the user should use the previous profile with new path name.

Event ID 300 - Windows Hello successfully created

Article • 09/02/2022 • 2 minutes to read

This event is created when Windows Hello for Business is successfully created and registered with Azure Active Directory (Azure AD). Applications or services can trigger actions on this event. For example, a certificate provisioning service can listen to this event and trigger a certificate request.

Applies to: Windows 10, Windows 11

Event details

Product: Windows 10 or Windows 11 operating system
Log: Event Viewer > Applications and Service Logs\Microsoft\Windows\User Device Registration\Admin
ID: 300
Source: Microsoft Azure Device Registration Service
Version: 10 or 11
Message: The NGC key was successfully registered. Key ID: {4476694e-8e3b-4ef8-8487-be21f95e6f07}. UPN:test@contoso.com. Attestation: ATT_SOFT. Client request ID: .
Server request ID: db2da6bd-3d70-4b9b-b26b-444f669902da.
Server response: {"kid":"4476694e-8e3b-4ef8-8487-be21f95e6f07","upn":"test@contoso.com"}

Resolution

This is a normal condition. No further action is required.

More information

- Windows Hello for Business
- How Windows Hello for Business works
- Manage Windows Hello for Business in your organization
- Why a PIN is better than a password
- Prepare people to use Windows Hello
- Windows Hello and password changes
- Windows Hello errors during PIN creation

- Windows Hello biometrics in the enterprise

Windows Hello errors during PIN creation

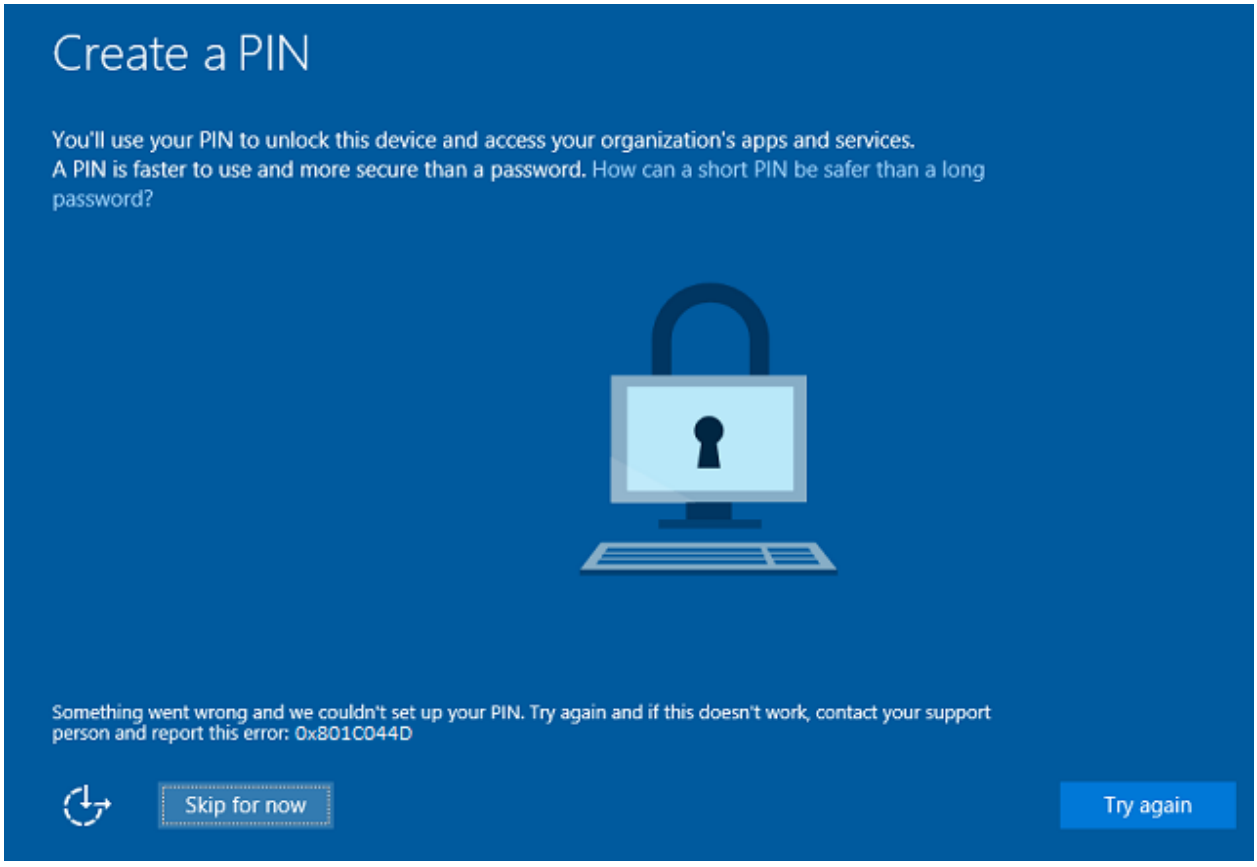
Article • 09/02/2022 • 5 minutes to read

When you set up Windows Hello in Windows client, you may get an error during the **Create a PIN** step. This article lists some of the error codes with recommendations for mitigating the problem. If you get an error code that isn't listed here, contact Microsoft Support.

Applies to: Windows 10, Windows 11

Where is the error code?

The following image shows an example of an error during **Create a PIN**.



Error mitigations

When a user encounters an error when creating the work PIN, advise the user to try the following steps. Many errors can be mitigated by one of these steps.

1. Try to create the PIN again. Some errors are transient and resolve themselves.

2. Sign out, sign in, and try to create the PIN again.
3. Reboot the device and then try to create the PIN again.
4. Unjoin the device from Azure Active Directory (Azure AD), rejoin, and then try to create the PIN again. To unjoin a device, go to **Settings** > **System** > **About** > **Disconnect from organization**.

If the error occurs again, check the error code against the following table to see if there's another mitigation for that error. When no mitigation is listed in the table, contact Microsoft Support for assistance.

Hex	Cause	Mitigation
0x80090005	NTE_BAD_DATA	Unjoin the device from Azure AD and rejoin.
0x8009000F	The container or key already exists.	Unjoin the device from Azure AD and rejoin.
0x80090011	The container or key was not found.	Unjoin the device from Azure AD and rejoin.
0x80090029	TPM is not set up.	Sign on with an administrator account. Select **Start**, type "*tpm.msc*", and select **tpm.msc Microsoft Common Console Document**. In the **Actions** pane, select **Prepare the TPM**.
0x8009002A	NTE_NO_MEMORY	Close programs which are taking up memory and try again.
0x80090031	NTE_AUTHENTICATION_IGNORED	Reboot the device. If the error occurs again after rebooting, reset the TPM or run Clear-TPM.
0x80090035	Policy requires TPM and the device does not have TPM.	Change the Windows Hello for Business policy to not require a TPM.
0x80090036	User canceled an interactive dialog.	User will be asked to try again.
0x801C0003	User is not authorized to enroll.	Check if the user has permission to perform the operation.
0x801C000E	Registration quota reached.	Unjoin some other device that is currently joined using the same account or increase the maximum number of devices per user.
0x801C000F	Operation successful, but the device requires a reboot.	Reboot the device.
0x801C0010	The AIK certificate is not valid or trusted.	Sign out and then sign in again.

Hex	Cause	Mitigation
0x801C0011	The attestation statement of the transport key is invalid.	Sign out and then sign in again.
0x801C0012	Discovery request is not in a valid format.	Sign out and then sign in again.
0x801C0015	The device is required to be joined to an Active Directory domain.	Join the device to an Active Directory domain.
0x801C0016	The federation provider configuration is empty	Go to http://clientconfig.microsoftonline-p.net/FPURL.xml and verify that the file is not empty.
0x801C0017	The federation provider domain is empty	Go to http://clientconfig.microsoftonline-p.net/FPURL.xml and verify that the FPDOMAINNAME element is not empty.
0x801C0018	The federation provider client configuration URL is empty	Go to http://clientconfig.microsoftonline-p.net/FPURL.xml and verify that the CLIENTCONFIG element contains a valid URL.
0x801C03E9	Server response message is invalid	Sign out and then sign in again.
0x801C03EA	Server failed to authorize user or device.	Check if the token is valid and user has permission to register Windows Hello for Business keys.
0x801C03EB	Server response http status is not valid	Sign out and then sign in again.
0x801C03EC	Unhandled exception from server.	sign out and then sign in again.

Hex	Cause	Mitigation
0x801C03ED	Multi-factor authentication is required for a 'ProvisionKey' operation, but was not performed. -or- Token was not found in the Authorization header. -or- Failed to read one or more objects. -or- The request sent to the server was invalid. -or- User does not have permissions to join to Azure AD.	Sign out and then sign in again. If that doesn't resolve the issue, unjoin the device from Azure AD and rejoin. Allow user(s) to join to Azure AD under Azure AD Device settings.
0x801C03EE	Attestation failed.	Sign out and then sign in again.
0x801C03EF	The AIK certificate is no longer valid.	Sign out and then sign in again.
0x801C03F2	Windows Hello key registration failed.	ERROR_BAD_DIRECTORY_REQUEST. Another object with the same value for property proxyAddresses already exists. To resolve the issue, refer to Duplicate Attributes Prevent Dirsync. Also, if no sync conflict exists, verify that the "Mail/Email address" in Azure Active Directory and the Primary SMTP address are the same in the proxy address.
0x801C044D	Authorization token does not contain device ID.	Unjoin the device from Azure AD and rejoin.
	Unable to obtain user token.	Sign out and then sign in again. Check network and credentials.
0x801C044E	Failed to receive user credentials input.	Sign out and then sign in again.

Hex	Cause	Mitigation
0xC00000BB	Your PIN or this option is temporarily unavailable.	The destination domain controller doesn't support the login method. Most often the KDC service doesn't have the proper certificate to support the login. Use a different login method.

Errors with unknown mitigation

For errors listed in this table, contact Microsoft Support for assistance.

Hex	Cause
0x80070057	Invalid parameter or argument is passed.
0X80072F0C	Unknown
0x80072F8F	A mismatch happens between the system's clock and the activation server's clock when attempting to activate Windows.
0x80090010	NTE_PERM
0x80090020	NTE_FAIL
0x80090027	Caller provided a wrong parameter. If third-party code receives this error, they must change their code.
0x8009002D	NTE_INTERNAL_ERROR
0x801C0001	ADRS server response is not in a valid format.
0x801C0002	Server failed to authenticate the user.
0x801C0006	Unhandled exception from server.
0x801C000B	Redirection is needed and redirected location is not a well known server.
0x801C000C	Discovery failed.
0x801C0013	Tenant ID is not found in the token.
0x801C0014	User SID is not found in the token.
0x801C0019	The federation provider client configuration is empty
0x801C001A	The DRS endpoint in the federation provider client configuration is empty.
0x801C001B	The device certificate is not found.

Hex	Cause
0x801C03F0	There is no key registered for the user.
0x801C03F1	There is no UPN in the token.
0x801C044C	There is no core window for the current thread.
0x801c004D	DSREG_NO_DEFAULT_ACCOUNT: NGC provisioning is unable to find the default WAM account to use to request Azure Active Directory token for provisioning. Unable to enroll a device to use a PIN for login.

More information

- Windows Hello for Business
- How Windows Hello for Business works
- Manage Windows Hello for Business in your organization
- Why a PIN is better than a password
- Prepare people to use Windows Hello
- Windows Hello and password changes
- Event ID 300 - Windows Hello successfully created
- Windows Hello biometrics in the enterprise

Virtualization troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Virtualization-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Virtualization sub categories

- Configuration of virtual machine settings
- Hyper-V Network Virtualization (HNV)
- Installation and configuration of Hyper-V
- Virtual machine creation
- Virtual machine performance

Office prompts for activation in Azure

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an issue where Microsoft Office applications prompt for reactivation when they are installed on Windows-based virtual machines in Azure.

Applies to: Windows 10 - all editions
Original KB number: 2998147

Symptoms

Office applications prompt for reactivation when they are installed on Windows-based virtual machines in Azure.

Cause

Azure automatically activates Microsoft Windows Servers by using an internal KMS (key management system) infrastructure within the Azure datacenters. Only virtual computers that are running in Azure can connect to and activate by using these KMS servers. The KMS servers let you activate Windows Server 2008 R2 and later versions. However, they do not include the Microsoft Office KMS activation packs.

As virtual machines migrate to new hosts during regular maintenance and certain administrative functions such as resizing or starting from the Stopped Deallocated state, Microsoft Office may prompt for reactivation if you are not using KMS, and instead you are using MAK (multiple activation keys). Over time, the operating system will detect multiple hardware changes, eventually causing Microsoft Office to require reactivation for this configuration.

Resolution

Microsoft Office is only permitted to be hosted in Azure under specific Service Provider agreements. Therefore, the Azure hosted KMS servers will not activate Microsoft Office applications automatically.

For environments that do have the correct licensing to host Microsoft Office, the recommended configuration is to leverage Active Directory Based Activation (if deploying Office 2013). If you are not deploying Office 2013 or cannot use Active Directory Based Activation, another option is to install a KMS host within the same virtual network as the hosted virtual machines in Azure or enable access to an on-

premise KMS host through a site-to-site tunnel. See the Office 2013 Volume Activation guide for KMS configuration.

More information

For more information about licensing software in Azure, reference the Virtual Machine Volume Licensing FAQ

For more information about how to apply for service provider licensing, reference the Volume Licensing Product Reference

Can't create a Hyper-V virtual switch on 64-bit versions of Windows 10

Article • 12/06/2021 • 2 minutes to read

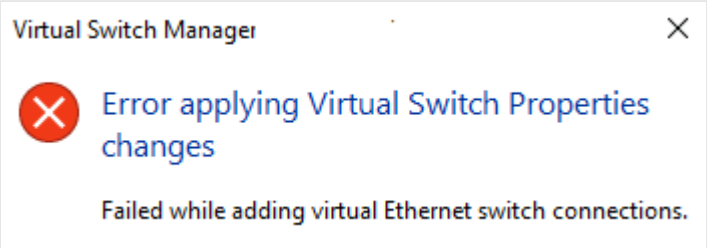
This article solves an error message when you try to re-create a Hyper-V virtual switch (vSwitch) for the same physical adapter.

Applies to: Windows 10 - all editions
Original KB number: 3101106

Symptoms

After you delete a vSwitch on a computer that has been upgraded to Windows 10, you can't re-create the vSwitch for the same physical adapter. When this problem occurs, you receive the following error message:

> Virtual Switch Manager
> Error applying Virtual Switch Properties changes
> Failed while adding virtual Ethernet switch connections.



It indicates that the vSwitch still exists, even though it's no longer listed in the Hyper-V Virtual Switch Manager.

Cause

This problem occurs because a new network setup functionality introduced in Windows 10 doesn't completely delete all objects from the previous vSwitch installation. This problem is scheduled to be fixed in the next Windows 10 update.

Resolution

To fix this problem automatically, select the following Download link. In the **File Download** dialog box, select **Run** or **Open**, and then follow the steps in the Easy fix wizard.

Download

Important

Before you run the Easy fix, note the following points:

- You will lose network connectivity after the wizard finishes.
- You must restart your computer manually after the wizard finishes.
- You will have to connect manually to all known Wi-Fi networks after your computer restarts.
- You must re-create the vSwitch by using the Hyper-V Virtual Switch Manager after your computer restarts.

Note

- This wizard may be in English only. However, the automatic fix also works for other language versions of Windows.
- If you are not on the computer that has the problem, save the Easy fix solution to a flash drive or a CD, and then run it on the computer that has the problem.

Can't use kdump or kexec for Linux virtual machines on Hyper-V

Article • 12/02/2021 • 3 minutes to read

This article provides a resolution to an issue where kdump or kexec can't be used for Linux virtual machines on Hyper-V.

Applies to: Windows Server 2012 R2, Windows Server 2008 R2 Service Pack 1
Original KB number: 2858695

Symptoms

- Pre-Windows Server 2012 R2

  Consider the following scenario:

  - You have a pre-Windows Server 2012 R2-based computer that has the Hyper-V role installed.
  - You install Linux on a Hyper-V virtual machine on the computer.
  - You configure kdump on the Linux virtual machine.

    > **Note**
    >
    > The Linux virtual machine already has the Linux Integration Services drivers. The drivers can be either prebuilt or manually installed.

    In this scenario, if the Linux virtual machine crashes, the core dump file from the Linux kernel is not generated as expected.

- Windows Server 2012 R2

  Consider the following scenario:

  - You have Linux virtual machines on Windows Server 2012 R2 Hyper-V host.
  - 15 or more vCPUs are attached to the Linux virtual machine.
  - You configure kdump in the Linux virtual machine.

In this scenario, kdump does not work, and the crash dump is not created, because the process stops responding (hangs).

Cause

This issue occurs because Hyper-V can't host two simultaneous connections from the same synthetic driver, which is running inside a virtual machine.

When kdump is configured on a Linux virtual machine that's using the Linux Integration Services synthetic storage driver (also known as storvsc), the kexec kernel is configured to use the same driver. If the Linux virtual machine crashes, the synthetic storage driver that's hosted in the kexec kernel tries to open a connection to the Hyper-V storage provider. However, Hyper-V fails to establish the new connection because of the pre-existing connection to the same storage driver on the crashed Linux virtual machine. Therefore, the kexec kernel cannot dump the core for the crashed Linux virtual machine.

Resolution

To resolve this issue, configure the kexec kernel by using the standard Linux storage driver. This configuration must be performed after the kdump functionality is enabled on a Linux virtual machine. The basic idea is to turn off the Linux Integration Services storage driver and then enable the standard Linux storage driver inside the kexec kernel by using the prefer_ms_hyper_v parameter in the appropriate configuration file.

The prefer_ms_hyper_v parameter can be used to control the behavior of the standard Linux storage driver. When this parameter is set to 1 and the Linux virtual machine is running on Hyper-V, the standard Linux storage driver disables itself and lets the Linux Integration Services storage driver control the storage devices. By setting the prefer_ms_hyper_v parameter to 0, the standard Linux storage driver is allowed to function. Because the standard Linux storage driver does not require a connection to Hyper-V, the kexec kernel can dump core.

Different Linux distributions have slightly different mechanisms to specify the value of prefer_ms_hyper_v. The following section describes how the parameter can be set for several popular Linux distributions.

Red Hat Enterprise Linux (RHEL)

In RHEL 5.9, you have to pass the **prefer_ms_hyper_v** parameter through a kernel command-line argument to the **ide_core** module that's built into the RHEL 5.9 kernel. By default, this parameter is initialized to 1, and it causes the Linux virtual machine to avoid

using the ide_core module if it's running in a Hyper-V environment. Administrators have to set the **prefer_ms_hyper_v** parameter value to 0 so that the ide_core driver becomes operational during the kexec kernel boot process.

In RHEL 6.4, you have to pass the **prefer_ms_hyper_v** parameter to the **ata_piix** driver module.

To do so, change the contents of /etc/kdump.conf. See 11.10. Preventing kernel drivers from loading for kdump for more information.

Ubuntu 12.04(.x)

In Ubuntu 12.04(. **x**), you have to pass the prefer_ms_hyper_v parameter to the ata_piix driver. You can do by changing the contents of the /etc/init.d/kdump file.

To change the contents of the /etc/init.d/kdump file, append ata_piix.prefer_ms_hyper_v=0 to the kdump command-line options:

Bash

```
do_start {}
{
    ....
    ....
    APPEND="$APPEND kdump_needed maxcpus=1 irqpoll reset_devices
ata_piix.prefer_ms_hyperv=0"
    ...
}
```

SUSE Linux Enterprise Server (SLES) 11 SP2(x)

In SLES 11 SP2(x) distributions, you have to pass the prefer_ms_hyper_v parameter to the ata_piix driver. You can do so by modifying the contents of the /etc/sysconfig/kdump file as follows:

Append ata_piix.prefer_ms_hyper_v=0 to KDUMP_COMMANDLINE_APPEND:

> KDUMP_COMMANDLINE_APPEND="ata_piix.prefer_ms_hyperv=0"

After the required edits, the /etc/sysconfig/kdump file looks like this:

> KDUMP_COMMANDLINE_APPEND="ata_piix.prefer_ms_hyperv=0"

More information

KDUMP should be configured in the standard manner that's suggested by Linux distributions.

Third-party information disclaimer

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

Supported Guest Operating Systems in Virtual PC

Article • 09/23/2021 • 2 minutes to read

This article provides some information about supported Guest Operating Systems in Virtual PC.

Applies to: Windows Server 2012 R2, Windows 7 Service Pack 1
Original KB number: 831461

Summary

This article discusses the operating systems that Windows Virtual PC supports.

More information

You can use the following operating systems as a guest operating system in a guest PC:

Operating System	Virtual PC 2007 32-bit	Windows Virtual PC 32-bit
Windows 7 Ultimate	No	Yes
Windows 7 Enterprise	No	Yes
Windows 7 Professional	No	Yes
Windows 7 Home Premium	No	Yes
Windows 7 Home Basic	No	Yes
Windows 7 Starter	No	No
Windows Server 2008 R2 (all editions)	No	No
Windows Vista Ultimate	Yes	Yes
Windows Vista Enterprise	Yes	Yes
Windows Vista Business	Yes	Yes
Windows Vista Home Premium	Yes	No
Windows Vista Home Basic	Yes	No
Windows Vista Starter	Yes	No

Operating System	Virtual PC 2007 32-bit	Windows Virtual PC 32-bit
Windows Server 2008 Standard Edition	Yes	No
Windows XP Professional	Yes	Yes
Windows XP Tablet PC Edition	Yes	No
Windows XP Media Center Edition	No	No
Windows XP Home Edition	Yes	No
Windows XP Starter	Yes	No
Windows Server 2003 Standard Edition	Yes	No

Additionally, you can install most x86-based operating systems in the Windows Virtual PC environment. For technical issues with third-party operating systems, contact the operating system vendor for support. Support for Microsoft operating systems whose lifecycles have ended may be limited or not available. Microsoft provides support for technical issues with the Windows Virtual PC program, regardless of the installed guest operating system.

Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft does not guarantee the accuracy of this third-party contact information.

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, regarding the performance or reliability of these products.

Hyper-V virtual machines don't start after you upgrade to Windows 10

Article • 12/06/2021 • 2 minutes to read

This article helps fix an issue where Windows 10 Hyper-V can't start virtual machines after a Windows 10 upgrade.

Applies to: Windows 10 - all editions
Original KB number: 4052082

Symptoms

Consider the following scenario:

- You have a Windows 10-based computer that has the Hyper-V role installed.
- You upgrade the computer to Windows 10, version 1709, Windows 10, version 1803, Windows 10, version 1809, Windows 10, version 1903 or Windows 10, version 1909.

In this scenario, you cannot start virtual machines. Also, you receive the following error message:

> Start-VM: 'VM_NAME' failed to start. (Virtual machine IDMachineID)
> 'VM_NAME' failed to start worker process: %%3228369022 (0xC06D007E). (Virtual machine IDMachineID)
> At line:1 char:1
> + Start-VM VM_NAME
> + ~~~~~~~~~~~~~~
> + CategoryInfo : NotSpecified: (:) [Start-VM], VirtualizationException
> + FullyQualifiedErrorId:
> OperationFailed,Microsoft.HyperV.PowerShell.Commands.StartVM

Additionally, you see the following entry in the System log:

> The Hyper-V Host Compute Service service terminated unexpectedly. It has done this 11 time(s).

And you see the following entry in the Application log:

Faulting application name: vmcompute.exe, version: 10.0.16299.15, time stamp: 0x1a906fe6
Faulting module name: vmcompute.exe, version: 10.0.16299.15, time stamp: 0x1a906fe6
Exception code: 0xc0000005
Fault offset: 0x000000000000474b
Faulting process id: 0x3d78
Faulting application start time: 0x01d34d80559647e6
Faulting application path: C:\WINDOWS\system32\vmcompute.exe
Faulting module path: C:\WINDOWS\system32\vmcompute.exe
Report Id: ReportID
Faulting package full name:
Faulting package-relative application ID:
Response: Not available
Cab Id: 0
Problem signature:
P1: vmcompute.exe
P2: 10.0.16299.15
P3: 1a906fe6
P4: vmcompute.exe
P5: 10.0.16299.15
P6: 1a906fe6
P7: c0000005
P8: 000000000000474b
P9:
P10:
Attached files:
\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER98A7.tmp.mdmp
\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER9974.tmp.WERInternalMetadata.xml
\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER9981.tmp.csv
\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER99C1.tmp.txt
\?\C:\Windows\Temp\WER99C3.tmp.appcompat.txt
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vmcompute.exe_101d36662442e0c1debf6dea58c1dd187cc5_51a43a19_cab_332099df\memory.hdmp \
These files may be available here:
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_vmcompute.exe_101d36662442e0c1debf6dea58c1dd187cc5_51a43a19_cab_332099df

> Analysis symbol:
> Rechecking for solution: 0
> Report Id:ReportID
> Report Status: 4
> Hashed bucket: \

Cause

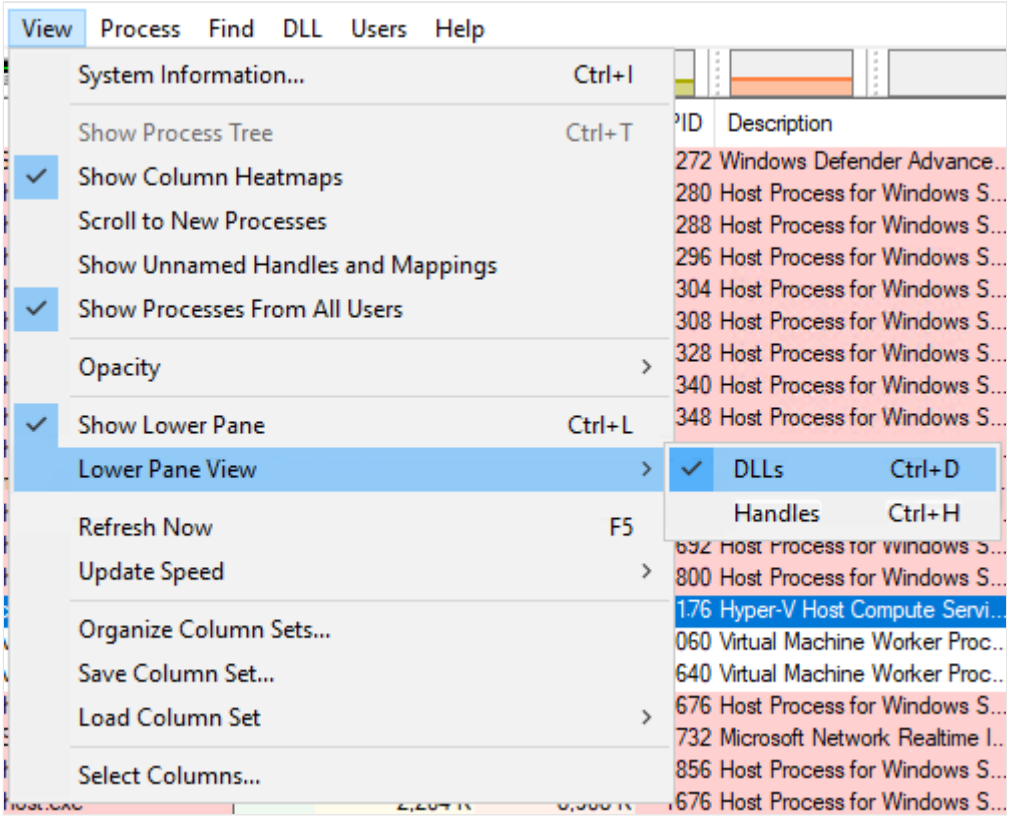
This issue occurs because Windows 10 enforces a policy that configures Vmcompute.exe not to allow any non-Microsoft DLL files to be loaded.

Resolution

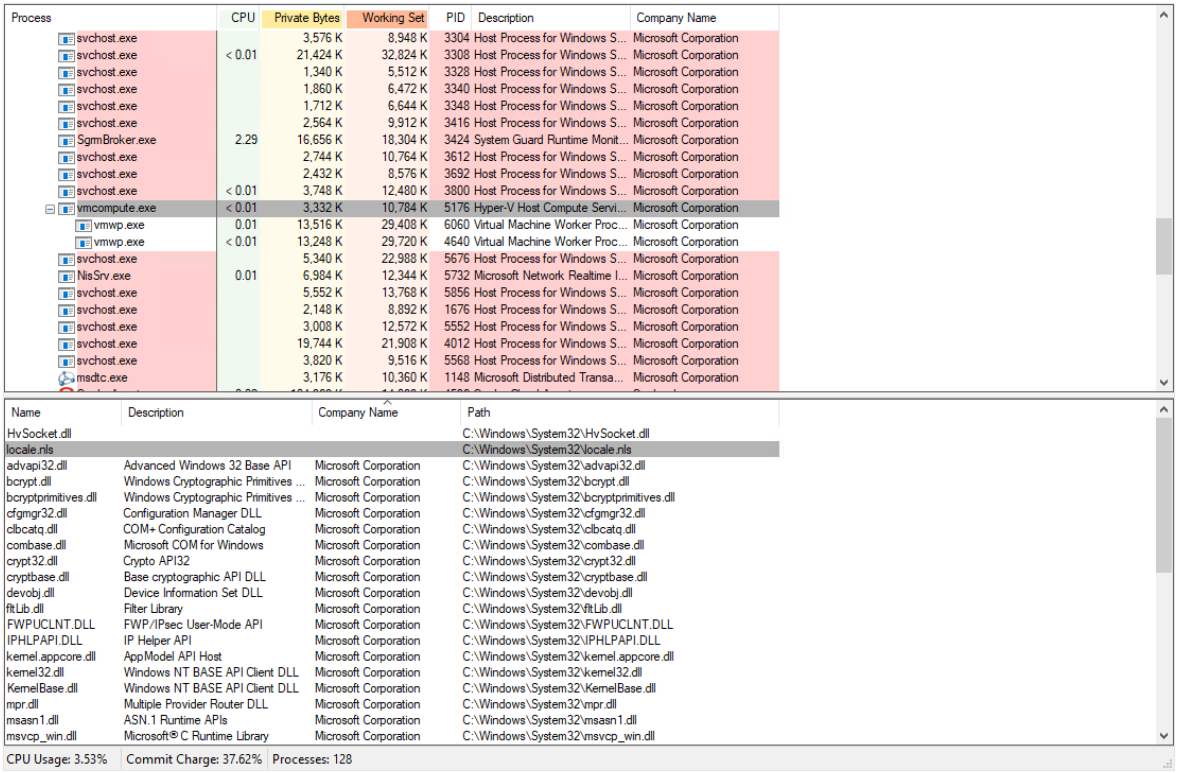
Vmcompute.exe process. One possible cause of this issue is your antivirus software.

To do this, you may use some tools such as process explorer. Follow these steps:

1. Download Process Explorer.
2. Extract the tool, and run ProcessExp64.exe, which is for 64-bit operating system.
3. Under **View** menu, select **Show Lower Pane**, click **Lower Pane View**, and then select **DLLs**.



4. Select the Vmcompute.exe process, and check for non-Microsoft DLLs in the lower pane. It is fine for some entries to be blank.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		3,576 K	8,948 K	3304	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	21,424 K	32,824 K	3308	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,340 K	5,512 K	3328	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,860 K	6,472 K	3340	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,712 K	6,644 K	3348	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,564 K	9,912 K	3416	Host Process for Windows S...	Microsoft Corporation
SgrmBroker.exe	2.29	16,656 K	18,304 K	3424	System Guard Runtime Monit...	Microsoft Corporation
svchost.exe		2,744 K	10,764 K	3612	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,432 K	8,576 K	3692	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	3,748 K	12,480 K	3800	Host Process for Windows S...	Microsoft Corporation
vmcompute.exe	< 0.01	3,332 K	10,784 K	5176	Hyper-V Host Compute Servi...	Microsoft Corporation
vmwp.exe	0.01	13,516 K	29,408 K	6060	Virtual Machine Worker Proc...	Microsoft Corporation
vmwp.exe	< 0.01	13,248 K	29,720 K	4640	Virtual Machine Worker Proc...	Microsoft Corporation
svchost.exe		5,340 K	22,988 K	5676	Host Process for Windows S...	Microsoft Corporation
NisSrv.exe	0.01	6,984 K	12,344 K	5732	Microsoft Network Realtime I...	Microsoft Corporation
svchost.exe		5,552 K	13,768 K	5856	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,148 K	8,892 K	1676	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,008 K	12,572 K	5552	Host Process for Windows S...	Microsoft Corporation
svchost.exe		19,744 K	21,908 K	4012	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,820 K	9,516 K	5568	Host Process for Windows S...	Microsoft Corporation
msdtc.exe		3,176 K	10,360 K	1148	Microsoft Distributed Transa...	Microsoft Corporation

Name	Description	Company Name	Path
HvSocket.dll			C:\Windows\System32\HvSocket.dll
locale.nls			C:\Windows\System32\locale.nls
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll
bcrypt.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcrypt.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\System32\cfgmgr32.dll
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\System32\clbcatq.dll
combase.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\combase.dll
crypt32.dll	Crypto API32	Microsoft Corporation	C:\Windows\System32\crypt32.dll
cryptbase.dll	Base cryptographic API DLL	Microsoft Corporation	C:\Windows\System32\cryptbase.dll
devobj.dll	Device Information Set DLL	Microsoft Corporation	C:\Windows\System32\devobj.dll
fltLib.dll	Filter Library	Microsoft Corporation	C:\Windows\System32\fltLib.dll
FWPUCLNT.DLL	FWP/IPsec User-Mode API	Microsoft Corporation	C:\Windows\System32\FWPUCLNT.DLL
IPHLPAPI.DLL	IP Helper API	Microsoft Corporation	C:\Windows\System32\IPHLPAPI.DLL
kernel.appcore.dll	AppModel API Host	Microsoft Corporation	C:\Windows\System32\kernel.appcore.dll
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\kernel32.dll
KernelBase.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\KernelBase.dll
mpr.dll	Multiple Provider Router DLL	Microsoft Corporation	C:\Windows\System32\mpr.dll
msasn1.dll	ASN.1 Runtime APIs	Microsoft Corporation	C:\Windows\System32\msasn1.dll
msvcp_win.dll	Microsoft® C Runtime Library	Microsoft Corporation	C:\Windows\System32\msvcp_win.dll

CPU Usage: 3.53% | Commit Charge: 37.62% | Processes: 128

Windows 7 EoS FAQ documentation

FAQ

This article summarizes the frequently asked questions about the end of support for Windows 7.

This article is intended for use by IT professionals. If you're looking for information for home users, see Windows 7 support ended on January 14, 2020 .

Applies to: Windows 7 Service Pack 1
Original KB number: 4527873

Windows 7 EoS FAQ

Get answers to common questions about the following end-of-support topics for Windows 7:

- General information
- FAQ about Extended Security Updates (ESU) for Windows 7
  - ESU purchasing
  - ESU coverage
  - ESU deployment
- Windows 7 ESU offers for E5 customers
- Troubleshoot issues in ESU

Frequently asked questions about the Windows 7 end of support

FAQ

This article describes the frequently asked questions about the end of support for Windows 7.

This article is intended for use by IT professionals. If you're looking for information for home users, see Windows 7 support will end on January 14, 2020.

Applies to: Windows 7 Service Pack 1
Original KB number: 4527875

When is the End of Support for Windows 7

Support for Windows 7 ended on January 14, 2020.

What does end of support mean

Microsoft Lifecycle Policy offers five years of Mainstream Support. Depending on the product, it also offers a period of Extended Support. For Windows operating systems, the Extended Support period is five years.

As defined in the policy, after the Extended Support period for a product ends, Microsoft no longer publishes updates or security updates for that product. This may create security and compliance issues and expose an organization's applications and business to serious security risks. Learn more at Microsoft Lifecycle Policy.

What is the recommended upgrade path for Windows 7 users

Recommended path: Enroll in Microsoft 365 or upgrade directly to the latest version of Windows 10. If you experience any application compatibility issues after you update to Windows 10, go to Desktop App Assure for assistance.

Fallback path: Enroll in Azure Virtual Desktop in Azure. After you enroll, you can get free Extended Security Updates to protect on-premises servers and desktops for three more

years.

Last resort path: Buy Extended Security Updates to protect on-premises servers and desktops for three more years.

If an organization can't transition from Windows 7 before the end of support deadline, what are its options

To help organizations protect data and applications during the end of support transition, especially those that can't complete the transition before the end-of-support date, we offer the following options:

- **Azure Virtual Desktop**. An appropriate option for organizations that can use a virtualization solution. Azure Virtual Desktop is the only cloud-based service that delivers a multi-user Windows 10 experience and is optimized for Microsoft 365 Apps for enterprise. This option includes free Windows 7 ESU.
- **Windows 7 Extended Security Updates (ESU)**. A last-resort option. Organizations can purchase Windows 7 ESU for their devices. ESU are also available for Windows Server 2008, Windows Server 2008 R2, SQL Server 2008, and SQL Server 2008 R2. For more information about Windows Server ESU offerings, see Extended Security Updates frequently asked questions.

ESU aren't available for Office 2010.

What assistance is available for organizations that are affected by the end of support for Windows 7

To help reduce security risks and continue to get regular security updates, we recommend that you upgrade to the latest versions of our software in the cloud.

- If your organization has access to cloud transition SKUs or Software Assurance (SA), talk to your account manager about your transition path. The Microsoft FastTrack program includes a large portfolio of deployment offers and tools that can help you reduce the time and cost that you require to upgrade. This portfolio includes remediation services such as Desktop App assure, Desktop Analytics, and others.

- If your organization doesn't have access to programs such as SA, talk to your account manager or Microsoft Partner about finding licensing offers that meet your needs.

What is Azure Virtual Desktop

Azure Virtual Desktop is a cloud-based service that is delivered on Azure. It's the best virtualized Windows and Office experience. It delivers a multi-user Windows 10 experience that is optimized for Microsoft 365 Apps for enterprise. For customers who are upgrading from Windows 7, Azure Virtual Desktop includes free Windows 7 ESU through 2023. You can use Azure Virtual Desktop to deploy and scale Windows and Office on Azure in minutes, including appropriate security and compliance measures.

When is Azure Virtual Desktop an appropriate solution

Azure Virtual Desktop is an appropriate option for organizations that can use a virtualization solution. Azure Virtual Desktop delivers a multi-user Windows 10 experience that is optimized for Microsoft 365 Apps for enterprise. For customers who are upgrading from Windows 7, Azure Virtual Desktop includes free Windows 7 ESU through 2023.

Where can I find information about the end of support for Windows Server 2008 or Windows 2008 R2

Support for Windows Server 2008 and Windows Server 2008 R2 ended on January 14, 2020. Learn more here.

What happens to Windows 7 virtual machines (VMs) that are hosted on Azure after January 2023? Will Microsoft remove them

Organizations that have Windows 7 VMs in Azure will continue to have access to those VMs after January 2023. Microsoft won't delete those VMs or block access to them. However, Microsoft will stop maintaining those VMs through updates. Therefore, the affected VMs will quickly fall out of compliance.

If an organization experiences an issue that requires a new feature, what support can the organization expect

We'll investigate the issue. If the issue can be resolved by a product enhancement that is available in a recent release, we recommend that the organization upgrade to that release (or a later release).

What tools and programs are available for organizations that have application compatibility concerns in moving from Windows 7 to Windows 10

Windows Autopilot simplifies the process of deploying new Windows 10 devices by providing an alternative to creating, maintaining, and loading custom images. Windows Autopilot lets you deliver new off-the-shelf Windows 10 devices directly to your users. Through a few simple clicks, the device transforms into a fully business-ready state, dramatically reducing the time required to get users up and running on new devices.

For more information, see Simplifying IT with the latest updates from Windows Autopilot.

Desktop Analytics is a cloud-based service that integrates with Configuration Manager. The service provides insight and intelligence for you to make more informed decisions about the update readiness of your Windows clients. It combines data from your organization with data aggregated from millions of devices connected to Microsoft cloud services. For more information, see What is Desktop Analytics?.

FastTrack deployment guidance for Windows 10 helps you to envision a technical plan, determine how to onboard and deploy new services and users, and provides support as you deploy to get the most value out of your technology investments. This assistance is

available at no additional cost for those who have 150 or more licenses of an eligible service or plan. For more information, see FastTrack Center Benefit for Windows 10.

App Assure service from FastTrack is a new service from Microsoft FastTrack that is designed to address app compatibility issues for Windows 10, Microsoft 365 Apps for enterprise, and Microsoft Edge. If you find any app compatibility issues after you update to Microsoft 365 Apps for enterprise or Windows 10, or after you switch to Edge from Internet Explorer or Chrome (including issues about macros and add-ins), App Assure helps you fix them. Simply let us know by filing a FastTrack ticket, and a Microsoft engineer will follow up to work with you until the issue is resolved.

Ready for Microsoft 365: The Ready for Microsoft 365 directory lists software solutions that are supported and in use on commercial devices running Windows 10 and Microsoft 365 Apps for enterprise. The directory is intended for IT managers at companies and organizations worldwide who are considering the latest versions of Windows 10 and Office 365 for their deployments.

What happens if I use Microsoft 365 Apps for enterprise on Windows 7

After January 2020, if you use Microsoft 365 Apps for enterprise on a Windows 7-based computer, Microsoft 365 Apps for enterprise won't receive any new feature updates. However, to provide some more time to make the transition to Windows 10 or other supported Windows operating system, Microsoft 365 Apps for enterprise will receive security updates through 2023.

Windows 7 ESU will have no effect on support for Microsoft 365 Apps for enterprise on Windows 7. Office 365 is governed by the Modern Lifecycle Policy that requires organizations to stay current per the servicing and system requirements for the product or service. These requirements include using Microsoft 365 Apps for enterprise on a Windows operating system that is currently in support.

We strongly advise against using Microsoft 365 Apps for enterprise on Windows 7. Using a modern cloud-backed client on an older, unsupported operating system may, over time, cause performance and reliability issues. Learn more about the relationship between Microsoft 365 Apps for enterprise and Windows 7 end of support.

> **Note**
>
> This information also applies to Office 365 Business. This is the version of Office that is included together with certain business plans, such as the Microsoft 365

Business and Office 365 Business Premium.

Why did some users in my organization receive a notification about Windows 7

Support for Windows 7 ended on January 14, 2020. Windows 7 users may receive notifications to remind them that their device is no longer supported and is no longer receiving security updates.

We designed these notifications so that they wouldn't appear on devices in managed organizations. More specifically, notifications are designed to exclude devices that have the following characteristics:

- Devices that run Enterprise or Server editions of Windows 7
- Devices that run any edition of Windows 7 from a Volume Licensing program
- Domain-joined devices
- Devices that operate in kiosk mode
- Devices on which registry settings restrict free upgrade notifications

Any devices in your organization that aren't covered by the listed criteria would see a notification. For more information about notifications, see You received a notification, "Your Windows 7 PC is out of support."

Did Windows 7 devices receive security updates on January 14, 2020

Updates were released on January 14, 2020 and all Windows 7 devices were eligible for those updates. Any security updates released after the end of support date apply only to Windows 7 devices that are covered by Windows 7 ESU.

FAQ about Windows 7 ESU

FAQ

This article describes the frequently asked questions about the extended security updates for Windows 7.

This article is intended for use by IT professionals. If you're looking for information for home users, see Windows 7 support ended on January 14, 2020 .

Applies to: Windows 7 Service Pack 1
Original KB number: 4527878

General information

What do Windows 7 ESU include?

Windows 7 Extended Security Updates (ESU) include security updates for critical and important issues as defined by Microsoft Security Response Center (MSRC) for a maximum of three years after January 14, 2020. After January 14, 2020, if your PC is running Windows 7, and you haven't purchased Extended Security Updates, the computer will no longer receive security updates.

> **Note**
>
> There won't be an ESU offering or an extension of support for Office 2010.

Which editions of Windows 7 are eligible for ESU?

ESU is available for Windows 7 Professional and Windows 7 Enterprise.

When will the ESU offer be available?

ESU has been available in the Volume Licensing Service Center (VLSC) since April 1, 2019, and from Cloud Solution Providers (CSPs) since Monday, December 2, 2019.

Where can I find out more about purchasing and installing Windows 7 ESU in Year 2?

The process for purchasing and installing ESU in Year 2 is identical to the process for Year 1. For more information, see Year two of Extended Security Updates for Windows 7 and Windows Server 2008 .

Do Windows 7 Embedded products qualify for Windows 7 ESU?

To obtain Windows 7 ESU for Windows 7 Embedded products, you have to have an Ecosystem Partner Servicing Offering (EPSO) support contract. You can't purchase Embedded ESU through Volume Licensing. Extended Support end dates for Windows 7 Embedded vary by edition. For more information, go to the following websites:

- Windows 7 for Embedded System (FES)
- Windows Embedded Standard 7 (WES)
- Windows Embedded POS Ready 7

Direct requests for ESU for Windows Server 2008 R2 for Embedded Systems and SQL Server 2008 R2 for Embedded Systems to the original manufacturer (OEM) of the device.

ESU purchasing

Is there a deadline for organizations to purchase ESU for Windows 7?

Organizations can purchase ESU at any time during the three years that the offer is available (2020, 2021, and 2022). If an organization waits and purchases ESU for the first time in year two or year three, they'll also have to pay for the preceding years. It's because the security updates that are offered under the ESU program are cumulative.

Although organizations can purchase ESU at any time, they won't have received bug fixes or security updates since January 14, 2020 without ESU. Additionally, Microsoft Support no longer provides any form of support for these customers.

If an organization waits and purchases ESU for the first time in Year 2 or Year 3, do they have to

purchase licenses for the preceding year(s) as well?

Yes. Because the updates are cumulative, organizations must pay for the preceding years if they purchase Windows 7 ESU for the first time in year two or year three. That is, customers must have purchased coverage for year 1 of ESU in order to buy year 2, and coverage for year 2 in order to buy year 3. Customers may buy coverage for previous years at the same time they buy coverage for a current period. It's unnecessary to buy a certain period of coverage within that coverage period.

How does the ESU purchasing transaction work for CSP Partners?

CSP Partners can find Windows 7 ESU offerings in the Partner Center purchase experience, on the subscription software price list under **Software**. For specific instructions to purchase ESU through Partner Center, see Purchasing Windows 7 ESU through a Cloud Solution Provider.

If a customer purchases Windows 7 ESU 2021 through CSP and changes their mind about the ESU purchase, are there any limitations on returns?

Yes. Windows 7 ESU 2021 returns through CSP can only be processed after the Year 2 coverage period starts on January 13, 2021. After January 13, 2021, CSP partners can request refunds for ESU purchases.

How can EDU customers purchase Windows 7 ESU?

Customers who own Windows 7 for Education (EDU) can purchase the commercial ESU offering from CSPs.

Who should I contact for more information about pricing and ordering for Windows 7 ESU?

VL customers: Contact your Account Team CE for pricing and ordering information that is tailored to specific customer scenarios.

Customers who are interested in purchasing Windows 7 ESU in CSP should reach out to a CSP partner. You can find a qualified partner at this site.

What is the SKU called in CSP?

The "Windows 7 Extended Security Updates 2020" SKU is available on the CSP price list.

Does Windows 7 ESU renew automatically for year two?

No. Windows 7 ESU will be made available as a separate SKU for each of the years in which it's offered (2020, 2021, and 2022). To continue ESU coverage, customers will have to separately purchase the SKU for each year.

Additional, in order to install Year two SKU, customers must purchase the Year one SKU. Installation and activation of the Year one SKU is not required.

What are the coverage dates for the three Windows 7 ESU SKUs?

- Windows 7 Extended Security Updates 2020: January 14, 2020 - January 12, 2021
- Windows 7 Extended Security Updates 2021: January 13, 2021 - January 11, 2022
- Windows 7 Extended Security Updates 2022: January 12, 2022 - January 10, 2023

For more information, see Lifecycle FAQ-Extended Security Updates.

Is there a minimum purchase requirement for Windows 7 ESU?

No. There are no minimum purchase requirements for Windows 7 ESU.

Is Software Assurance (SA) required to take advantage of ESU?

No. However, VL customers who have subscription licenses for Windows Enterprise SA or Windows Enterprise E3 receive advantageous pricing.
Are there any plans to release a separate Windows 7 ESU SKU for CSP customers who have active Software Assurance?

No.

How will licensing work for Windows 7 ESU in virtual machine environments?

ESU is licensed per device. For traditional on-premises or dedicated Virtual Desktop Infrastructure (VDI), each endpoint that accesses a VM that runs Windows 7 ESU must have an ESU license. In other words, it's not the VMs that must be counted, but the terminals. If the customer moves to Azure Virtual Desktop (AVD), ESU is covered for no extra cost for the full three-year coverage period.

Will ESU be available through Unified Support?

No. ESU is available to purchase only through VL and CSP.

Will ESU be available through the Microsoft Products & Services Agreement (MPSA)?

No. ESU is out-of-scope for MPSA.

I purchased Windows 7 ESU and this purchase isn't on the invoice for the same calendar month. Why dose it happen?

If you purchase Windows 7 ESU before the monthly invoice generation date, the purchase will be shown on the previous month's invoice. It won't be shown on the current calendar month's invoice.

For example, in March, if CSP purchased ESU before March 6, the purchase would show on February's invoice.

ESU coverage

Does this offer also apply to Windows XP, Windows Vista, or earlier versions?

Windows XP and Windows Vista support has already ended, and no further support is available. Customers are encouraged to move to Windows 10 to take advantage of the latest in security and reliability.

Will the Windows 7 ESU include updates for .NET Framework? If so, which version?

Yes. Windows 7 ESU will include support for the .NET Framework 4.5.2-4.8 releases (as of January 2020) and .NET Framework 3.5 Service Pack 1 (SP1). .NET Framework 4.5.2, 4.6, and 4.6.1 will reach end of support on April 26, 2022. After this date, Windows 7 ESU will include .NET Framework 4.6.2 through 4.8 and .NET Framework 3.5 SP1 only.

Do Windows 7 Embedded products qualify?

Yes, there's an ESU program specifically for embedded devices. For more information, see ESU for Windows 7 Embedded.

Can Windows 7 Pro OEM customers purchase Windows 7 ESU?

Yes.

Windows 7 VMs hosted in Azure receive free ESU. How are updates delivered to these VMs?

ESU for Windows 7 VMs on Azure is delivered by using the same methods as for on-premises clients. For more information, see the ESU deployment section in this article.

Will Microsoft Security Essentials (MSE) continue to protect my computer after end of support?

Microsoft Security Essentials (MSE) will continue to receive signature updates after January 14, 2020. However, the MSE platform will no longer be updated. Learn more about MSE.

Are System Center Endpoint Protection (SCEP) Virus Definition updates for Windows 7 covered by ESU?

SCEP definition and engine updates will continue for Windows 7 regardless of ESU status, according to the respective lifecycle policy for the listed SCEP versions.

- All in-support versions of SCEP offer anti-spyware and anti-virus updates on version 4.10.209.
- SCEP Current Branch will be the only EndPoint Protection product that will offer AV updates (until January 2023) after the 2012 version reaches its end of support in July 2022.

Is technical support included?

No. Customers that purchase directly from Microsoft (for example, VL customers or CSP direct Partners) can use an active support contract, such as Software Assurance or Premier or Unified Support, to request assistance with Windows 7. Partners can also use their Partner Support Plans to request assistance for Windows 7.

Can customers get technical support on-premises for Windows 7 after the end-of-support date if they do not purchase ESU?

No. If customers have Windows 7 and don't purchase ESU, they can't log support tickets for Windows 7, even if they have support plans.

Can an organization that purchases ESU use its Unified or Premier Support agreements to submit support incidents?

Yes. Organizations that use VL to purchase ESU can submit support incidents by using any Microsoft Support offering, including Unified and Premier Support.

Can customers use their Premier/Unified contracts to contact support if they have purchased ESU from a CSP Partner?

No. CSP customers should use their partners for technical support or purchase a pay-per-incident plan through Microsoft Professional support.

Can partners submit support incidents for their customers?

Yes. CSP direct Partners can use their existing Partner Support plans to request assistance for Windows 7 ESU if the customer has purchased ESU. Resellers should work together with their CSP indirect Partners to request assistance for Windows 7 questions regarding devices that are covered by ESU.

To locate your Tenant ID, sign in to `admin.microsoft.com` by using your organization administrator account. In the upper-left corner of the portal, select the app-launcher icon, and then select **Admin**. If you don't see the Admin tile, you don't have the correct permissions to access the admin center for your organization. Typically, your organization's network administrator or IT administrator have these permissions.

How are ESU customers entitled for support? Can they submit tickets online by using Microsoft Support or Services Hub?

All ESU customers must call Microsoft Support in order to place a request for a technical support incident. Premier and Unified customers can find the correct number to call within Services Hub. Non-Premier and Unified customers can find the correct number to call on the Global Customer Service phone numbers page.

How does a Microsoft Support agent know who has purchased ESU?

We continue to work to fully automate the validation process. If a customer purchased ESU as part of their Enterprise Agreement, an agent can verify the purchase by asking for the customer's Enterprise Agreement number or for the full customer name. To locate their Agreement Number, a customer can sign in to Volume License Service Center, and go to **Licenses** > **License Summary**. Typically, the License Summary displays recently purchased licenses within 24 hours after Microsoft receives a customer order from a Microsoft Partner.

What type of response should customers expect if they encounter an issue that requires a new feature?

No new product enhancements will be made for Windows 7. ESU helps keep Windows 7 devices secure for a limited time, and assist customers during the transition to a supported version of Windows. If an investigation into a customer issue determines that a product enhancement in a recent release (such as Windows 10) resolves the issue,

Microsoft Support will recommend that the customers upgrade to the most recent release.

After customers purchase ESU, will Microsoft help troubleshoot issues that aren't related to an extended security update?

Because Windows 7 support has ended, Microsoft is committed to helping customers upgrade to a supported version of Windows or migrate to the cloud. We'll provide best-effort support to troubleshoot issues for customers who purchase Windows 7 ESU.

What type of response should customers expect when they request support for a product that is covered by ESU?

For VL customers and CSP direct partners who have Premier Support plans, the expectations are as follows.

Scenario	Response
Support Engineer will open a support ticket	Yes
Support Team will work to solve customer issue	Yes
Support Team will do a root cause analysis	No
Support Team will file a bug	No

Is Internet Explorer 11 covered under Windows 7 ESU?

Yes. Internet Explorer 11 will receive security updates as necessary through Windows 7 ESU.

When will security updates be delivered for customers who have purchased Windows 7 ESU?

Security updates for Windows 7 will be released to ESU customers on the second Tuesday of every month. If there are no Critical or Important updates for Windows 7 in any given month (as prescribed by the Microsoft Security Response Center), there will be no ESU updates in that update cycle. If an off-cycle security update is considered

necessary, Windows 7 ESU customers will receive the update outside the regular monthly cadence.

Is there any advance notification of security updates for Windows 7 ESU?

No. There's no advance notification of security updates for Windows 7 ESU at this time. However, you can view details of past updates at Windows 7 SP1 and Windows Server 2008 R2 SP1 update history.

Where can I learn more about the specific security updates that have been issued for Windows 7 ESU?

A full list of updates to Windows 7 SP1, including ESU updates, is available at Windows 7 SP1 and Windows Server 2008 R2 SP1 update history.

ESU deployment

Are there any prerequisites for deploying ESU?

Yes. Before a customer deploys ESU, they should read Obtaining Extended Security Updates for eligible Windows devices. That post provides detailed explanations of all prerequisites and detailed instructions for deployment.

How can organizations install and activate the Windows 7 ESU MAK key?

For instructions to install and activate the Windows 7 ESU Multiple Activation Key (MAK), and more information about purchasing, see Obtaining Extended Security Updates for eligible Windows devices.

For more information about how to install and activate Windows 7 ESU MAK keys on multiple devices in an on-premises Active Directory domain, see the following article:

Activate Windows 7 ESUs on multiple devices with a MAK.

> **Note**

Installing MAK keys adds the ability to receive ESU. It doesn't replace the current product activation key (for example, OEM, KMS), nor does it reactivate the system. Organizations will have to install a new MAK key for every year that they deploy ESU.

Do I need to uninstall the Windows 7 ESU Year 1 MAK key to install the Year 2 key?

No. Nothing needs to be done to the Year 1 key to install the Year 2 key. The installation process for Year 2 is identical to Year 1 (see previous question, above).

Can Windows 7 ESU Year 1 updates be applied to a device after January 12, 2021 if the Year 1 key is installed on the device?

Yes, updates can be installed at any time. That allows you to maintain your existing patch rollout process when the Year 1 key is installed and activated on a device. The same applies for Year 2 and Year 3. For more information, see What are the coverage dates for the three Windows 7 ESU SKUs.

Why are the ESU License Preparation Packages necessary?

The Extended Security Updates (ESU) License Preparation Packages (Extended Security Updates (ESU) Licensing Preparation Package for Windows 7 SP1 and Windows Server 2008 R2 SP1 and Extended Security Updates (ESU) Licensing Preparation Package for Windows Server 2008 SP2) address activation experience requirements that we identified while testing and evaluating by using a large population of preview customers. We introduced the ESU License Preparation Packages on February 11, 2020 to:

- provide a consistent user experience going forward
- minimize the number of package installations
- reduce overall customer disruption

How will Microsoft deliver ESU for organizations that purchase through volume licensing (VL)?

An organization that uses volume licensing (VL) to manage on-premises deployments can use VL to deploy ESU to the covered devices. When an organization purchases Windows 7 ESU, Microsoft provides a MAK key in the VLSC. This MAK key is independent of the Windows 7 activation key and won't interfere with the existing Key Management Server (KMS) operating system activation deployment.

Administrators can access the key within VLSC by selecting **Licenses** > **Relationship Summary** > **[Licensing ID]** > **Product Keys**.

> ⓘ **Note**
>
> In this path, **[Licensing ID]** refers to the licensing ID of the organization.

The product key list will include the ESU key, which is named **Windows 7 Ext Security Year 1 MAK**. Organizations can deploy the new MAK key and any prerequisite servicing stack updates to the applicable devices, then continue their typical update and servicing strategy to deploy ESU by using Windows Update, Windows Server Update Services (WSUS), or whatever update management solution the organization prefers. It is also the process that organizations have to follow to update Azure Stack. For more information about how to use MAK for VL customers, see the VLSC Product Keys FAQ.

Will organizations have to have a new MAK key for each of the three years that ESU is available?

Yes. Organizations have to purchase, install, and activate new keys for each of the three years.

How can I determine when my ESU key will expire?

The yearly ESU MAK keys don't expire. However, they don't enable the device to install updates beyond their designated time frame. For example, a device with only a Year 1 ESU MAK key can continue to install updates made available during Year 1 even after the Year 1 time frame ends. But it won't receive any further updates in Year 2.

If an organization has to reinstall Windows 7, how will the additional activation of ESU be managed?

- Organizations that purchase ESU through a Partner should go to the Partner to receive additional activations.
- Organizations that purchased ESU through VLSC should open a VLSC support case to make this request.

What delivery options are available for Extended Security Updates?

ESU is delivered through all the usual update delivery channels, including:

- Configuration Manager (current branch, version 1910 or later)
- Windows Update (WU)
- Windows Server Update Service (WSUS)
- Microsoft Update Catalog

The update is programmed to look for the MAK activation on the endpoint, and will install only on those systems together with the MAK key. Learn more about Extended Security Updates and Configuration Manager.

> **Note**
>
> The ESU License Preparation Packages (**Extended Security Updates (ESU) Licensing Preparation Package for Windows 7 SP1 and Windows Server 2008 R2 SP1** and **Extended Security Updates (ESU) Licensing Preparation Package for Windows Server 2008 SP2**) are available through all of the previously mentioned channels except Windows Update.

Is offline servicing available for operating system images that are covered by ESU?

No. The ESU for Windows 7 and Windows Server 2008 require online servicing (using audit mode to modify images).

ESU updates aren't supported in offline servicing mode. Applying ESU in offline servicing mode generates an error, and updates fail.

How can a customer learn how many activations are left on their ESU MAK key?

Customers can determine the remaining activations on an MAK key by using the Volume Activation Management Tool (VAMT):

1. Start the VAMT.
2. In the navigation pane, select the **Product Keys** node.
3. In the center pane, find the "ESU Add-on MAK" key. The remaining activation count is displayed in the **Remaining Activation Count** column.

Can VAMT be run on a virtual client?

Yes.

If VAMT is run on a virtual client for Windows 7 ESU deployment, does the VAMT host VM have to remain running after activating all the Windows 7 clients, or can it be decommissioned?

The VAMT host VM can be decommissioned after it activates all the Windows 7 ESU clients.

Will the number of activations that are available by using an ESU MAK key be limited?

Yes. The number of activations that are available will depend on the number of licenses that the customer has purchased and also the terms of that customer's specific licensing agreement.

The number of activations shown in VLSC is less than the number that our organization purchased. How can I request the correct number?

1. On the VLSC home page, select **Contact Us**.
2. Select your region, and then select **Support Web Form** in the **Contact Info** section.
3. In the form, fill out the required information.

If an organization needs additional activations of ESU (for example, if they have to reinstall Windows 7 or reimage a device), how will those additional activations be managed?

Organizations that purchase ESU through volume licensing should request additional activations through the VLSC:

1. On the VLSC home page, select **Contact Us**.
2. Select your region, and then select **Support Web Form** in the **Contact Info** section.
3. In the form, complete the required information.

Most organizations that purchase ESU through CSP shouldn't have to request additional activations. For exceptional scenarios in which additional activations are required, Partners should use Partner Center to open a support request.

Can customers activate Windows 7 ESU through a phone?

Yes. For detailed instructions, see Obtaining Extended Security Updates for eligible Windows devices.

ESU for Windows 7 Embedded

Do Windows 7 Embedded products qualify for ESU?

Yes, there is an ESU program specifically for embedded devices. This program includes:

- Windows 7 for Embedded Systems
- Windows Embedded Standard 7
- Windows Embedded POSReady 7

The ESU for Windows 7 Embedded also includes Windows Server 2008 R2 for Embedded Systems and Microsoft SQL Server 2008 R2 for Embedded Systems. Direct all embedded ESU requests to the original equipment manufacturer (OEM) of the device.

Where can I find more information about the embedded ESU program?

Contact your OEM for all Windows 7 Embedded ESU questions.

Why isn’t ESU for Windows Embedded Standard 7 available via CSP or volume licensing?

Windows Embedded Standard 7 is an embedded-only OS and is exclusively available from OEMs.

How much does ESU for Windows Embedded Standard 7 cost?

Contact your OEM for ESU pricing.

Will my customer’s devices running Windows Embedded Standard 7 be unprotected after October 13, 2020?

When security updates are available, Microsoft releases these monthly – on the second Tuesday of each month. If there are no critical or important updates released between October 14, 2020 and November 9, 2020, those devices will have the most current security updates from Microsoft. However, when the November 10, 2020 security updates are released, devices running WES will be unprotected and a security risk.

How are "critical" and "important" updates defined?

Visit by the Microsoft Security Response Center (MSRC) for more information on security update ratings: https://aka.ms/msrc_ratings .

FAQ about Windows 7 ESU offers for E5 customers

FAQ

This article describes the frequently asked questions about the Extended Security Updates offers for E5 customers for Windows 7.

This article is intended for use by IT professionals. If you're looking for information for home users, see Windows 7 support ended on January 14, 2020 .

Applies to: Windows 7 Service Pack 1
Original KB number: 4527879

Is Windows 7 Year 1 ESU included with Microsoft 365 E5?

Yes. Starting March 1, 2020, Microsoft is introducing a new program that includes Windows 7 Year 1 ESU together with Microsoft 365 E5, Microsoft 365 E5 Security, and Microsoft 365 Security + Compliance Subscription License.

In this new program, which subscriptions include Windows 7 Year 1 ESU?

- Microsoft 365 E5
- Microsoft 365 E5 Security
- Microsoft 365 Security + Compliance Subscription License (SL)

Who can take advantage of this program?

Windows 7 Year 1 ESU combined with Microsoft 365 E5 is available to Volume Licensing (VL) customers who purchase through EA or EAS agreements.

What are the effective dates of this program?

March 1, 2020 - December 31, 2020.

Do customers have to maintain Microsoft 365 E5 subscriptions throughout the ESU coverage period?

Yes. Customers must maintain the qualifying E5 SKUs through the end of the Windows 7 Year 1 ESU period (January 12, 2021) to benefit from the included ESU.

Why is only Windows 7 Year 1 ESU included?

We believe that most customers who have to purchase Windows 7 ESU require only Year 1 coverage as they continue to deploy Windows 10.

Troubleshoot issues in ESU

FAQ

This article describes emerging issues that affect Extended Security Updates (ESU) deployments and the steps to troubleshoot these issues. This information is organized by task, as follows:

- Installing update prerequisites
- Installing ESU keys
- Activating ESU keys
- Installing ESU
- Maintaining ongoing ESU compliance

Applies to: Windows Server 2012 R2, Windows 7 Service Pack 1
Original KB number: 4547184

Installing ESU prerequisites

You may experience the following issues when you install the ESU prerequisites.

The update isn't applicable to your computer

When you install an update that's required by ESU, you see a message similar to the following example:

> The update is not applicable to your computer.

Possible cause

The package that you're trying to install isn't applicable to your Windows operating system edition or architecture.

Actions to take

- Make sure that the package is meant for your operating system edition and architecture.
- Restart the computer, and then try to install the package again.
- If you still see the error message, see The update is not applicable to your computer.

Additional steps

If the preceding steps don't resolve the problem, follow these steps on the affected computer:

1. Copy the component-based servicing (CBS) log file (C:\Windows\Logs\CBS\CBS.log).
2. Contact Microsoft Support, and provide this log file.

Installer encountered an error: 0x80096010. The digital signature of the object did not verify

When you install an update that's required by ESU, you see a message similar to the following example:

> Installer encountered an error: 0x80096010.
> The digital signature of the object did not verify.

Possible cause

The computer is missing the SHA-2 updates.

Actions to take

Install the SHA-2 updates. For a list of prerequisites and SHA-2 updates, see the "Installation prerequisites" section of Obtaining Extended Security Updates for eligible Windows devices.

Installing ESU product activation keys

You may experience the following problems when you install a product activation key for ESU on a computer. This section assumes that all of the prerequisite updates for ESU are installed on the computer.

Run 'slui.exe 0x2a 0xC004F050' to display the error text. Error: 0xC004F050

When you install an ESU key, you see a message similar to the following example:

> Run 'slui.exe 0x2a 0xC004F050' to display the error text.
> Error: 0xC004F050

Possible causes

This problem may occur under any of the following conditions:

- The licensing monthly rollup/security only/standalone package isn't installed on the computer.
- The computer hasn't been restarted after installing the updates.
- Windows Server 2008 SP2-based computers sometimes require another restart.

Actions to take

1. Review the update history of the computer to make sure that all the ESU prerequisites have been installed successfully. For a list of the prerequisites, see Obtaining Extended Security Updates for eligible Windows devices.
2. Verify that the key that you're installing is the correct key for the computer and its operating system.
3. Restart the computer, and then install the key again.

Additional steps

If the preceding steps don't resolve the problem, follow these steps on the affected computer:

1. Copy the component-based servicing (CBS) log file (C:\Windows\Logs\CBS\CBS.log).
2. Contact Microsoft Support, and provide this log file.

Error: 0xC004F050 The Software Licensing Service reports that the product key is invalid

When you install the ESU product key by using `slmgr.vbs /ipk`, you receive the following Windows Script Host message:

> Error: 0xC004F050 The Software Licensing Service reported that the product key is invalid.

Cause

This problem can occur in either of the following circumstances:

- The licensing monthly rollup/security only/standalone package isn't installed on the computer.

- You installed the prerequisite updates, but you didn't restart the computer.

Actions to take

1. Check the computer's update history to make sure that all ESU prerequisite updates have been installed successfully.

   For a list of the required updates and information about how to get them, see Obtaining Extended Security Updates for eligible Windows devices.

2. Make sure that the key that you're installing is the correct key for the computer and its operating system.

3. Restart the computer, and try again.

Additional steps

If the preceding steps don't resolve the problem, follow these steps on the affected computer:

1. Copy the component-based servicing (CBS) log file (C:\Windows\Logs\CBS\CBS.log).
2. Contact Microsoft Support, and provide this log file.

The Software Licensing Service reports that the product key is invalid

When you add the ESU product key to the Volume Activation Management Tool (VAMT), you receive the following message:

> Unable to verify product key
> The specified product key is invalid, or is unsupported by this version of VAMT. An update to support additional products may be available online.

Cause

This issue can occur if two of the files that support VAMT aren't updated to support ESU keys.

Resolution

To fix this problem, update the VAMT configuration files with these steps:

1. Download the VAMT files. The download includes the following files:

    - pkconfig_win7.xrm-ms
    - pkconfig_vista.xrm-ms

2. Copy the two downloaded files to C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\VAMT3\pkconfig, replacing the older versions of the files.
3. Close VAMT, and then restart it.

The Software Licensing Service reports that the product key is invalid

When you use VAMT to install an ESU key on a computer, you receive the following Action Status message:

> The Software Licensing Service reports that the product key is invalid

Cause

This issue can occur if the computer is missing the prerequisite updates that ESU requires.

Resolution

For a list of the required updates and information about how to get them, see Obtaining Extended Security Updates for eligible Windows devices.

Activating ESU keys

You may experience the following problems when you activate the ESU key on a computer. This section assumes that the computer has the product activation key and all the prerequisite updates for ESU installed.

This section is divided into four parts. Some problems may occur during any type of activation, and some problems are specific to the activation type that your use.

Any activation method

Error: 0x80072F8F: Content decoding has failed

When you try to activate a Windows 7, Windows Server 2008, or Windows Server 2008 R2 ESU key, you receive the following error message:

> 0x80072F8F
> 147012721
> WININET_E_DECODING_FAILED
> Content decoding has failed

Cause

This issue may occur if TLS 1.0 is disabled and the `HKEY_LOCAL_MACHINE\System\CurrenteControlSet\Control\SecurityProviders\Schannel\Protocols\TLS 1.0\Client` subkey is set as follows:

- DisabledByDefault: 1
- Enabled: 0

Actions to take

This method forces the activation process to use TLS 1.2 by default so that TLS 1.0 can remain disabled.

To resolve this issue, follow these steps.

1. If update 3140245 isn't installed on the computer, use Windows Update to install it.
2. Open **regedit**, and navigate to the following registry subkey:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp`

   Create or set a **REG_DWORD** value of **DefaultSecureProtocols**, and set it to **0x800**.
3. If the computer is x64, you must also set the following registry key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp`

   Create or set a **REG_DWORD** value of **DefaultSecureProtocols**, and set it to **0x800**.
4. Restart the computer, and then try to run the `slmgr.vbs /ato` command again.

Slmgr activation

This section describes problems that you might experience when you use the Slmgr tool for activation.

Product activation failed while trying to activate ESU product key

When you try to activate the product key, you get a message similar to the following example:

> Error: Product activation failed.

Cause

The Windows operating system edition or architecture isn't eligible for ESU.

Actions to take

Make sure that the Windows operating system edition or architecture is in the list of editions and architectures that are supported for ESU. For a list, see Obtaining Extended Security Updates for eligible Windows devices.

Additional steps

If the preceding steps don't resolve the problem, contact Microsoft Support.

0xC004C020 the activation server reported that the Multiple Activation Key (MAK) has exceeded its limit

When you try to activate the product key, you get a message similar to the following example:

> 0xC004C020 the activation server reported that the Multiple Activation Key has exceeded its limit

Cause

A MAK supports a limited number of activations. In this case, the MAK has exceeded its activation limit.

Actions to take

To increase the number of activations that the MAK key supports, contact the Microsoft Licensing Activation Centers.

Product not found while trying to activate ESU key

When you activate the ESU product key, you receive a "product not found" message.

Cause

The activation ID that you used in the activation command isn't correct.

Actions to take

To get the activation ID, follow these steps:

1. Open an elevated Command Prompt window.
2. Run the following command: `cscript /h:cscript`.
3. Run one of the following commands, depending on your version of Windows.
    - For Windows 7: `slmgr /dlv`
    - For Windows Server 2008 SP2: `slmgr /dlv all`
4. In the command output, copy the activation ID of the ESU key.

To use the activation ID, run the following command: `slmgr /ato <Activation ID>`.

> **Note**
>
> In this command, <Activation ID> represents the activation ID of the ESU key.

0xC004F025 access denied: the requested action requires elevated privileges

When you try to activate the product key, you receive a message similar to the following example:

> 0xC004F025 access denied: the requested action requires elevated privileges.

Possible Cause

You may be using a regular Command Prompt window instead of an elevated Command Prompt window.

Actions to take

To open an elevated Command Prompt window:

- Select **Start**, right-click **Command Prompt**, and then select **Run as administrator**.

Error: 0x80072EE7

When you try to activate the product key, you receive a message similar to the following example:

> On a computer running Microsoft Windows non-core edition, run 'slui.exe 0x2a 0x80072EE7' to display the error text.
> Error: 0x80072EE7

Cause

The computer can't communicate with the Microsoft Activation and Validation Services (AVS) server to activate the ESU key.

Actions to take

Make sure that the computer is connected to the internet, or has the Activation URLs in the allow list, and try again.

For computers that don't connect directly to the internet, you can use VAMT Proxy activation or Phone activation as an alternative. For more information, see Obtaining Extended Security Updates for eligible Windows devices.

For the current VAMT Proxy Activation URLs, see the "Volume Activation Management Tool (VAMT) activation" section.

0x80072EE2 The operation timed out

When you try to activate the product key, you get a message similar to the following example:

> 0x80072EE2 The operation timed out

Possible causes

The computer can't connect to the Microsoft Activation service. It might not be connected to internet, or it might have issues with internet connectivity.

Actions to take

Make sure that the computer is connected to internet, or has the Activation URLs in the allow list, and try again.

For computers that don't connect directly to the internet, you can use VAMT Proxy activation or Phone activation as an alternative. For more information, see Obtaining Extended Security Updates for eligible Windows devices.

For the current VAMT Proxy Activation URLs, see the "Volume Activation Management Tool (VAMT) activation" section.

Activation command succeeds but the ESU key is still in Unlicensed state

You appear to have successfully activated the ESU key. However, the key still doesn't seem to be properly licensed.

Possible cause

The `slmgr /ato` command didn't correctly pass the ESU activation ID.

Action to take

To use the activation ID, run the following command: `slmgr /ato <Activation ID>`.

> **Note**
>
> In this command, <Activation ID> represents the activation ID of the ESU key.

License Status: Unlicensed

Collapsible element body

Volume Activation Management Tool (VAMT) activation

This section describes problems that you might experience when you use VAMT online or proxy activation. When you do so, use the following VAMT proxy activation URLs:

- `https://activation.sls.microsoft.com/BatchActivation/BatchActivation.asmx`
- `https://go.microsoft.com/fwlink/?LinkId=82160` (This FWLink redirects to the preceding URL.) Or, include the following domains in the computer's allow list:
- activation.sls.microsoft.com
- `go.microsoft.com`

Unable to verify product key

When you try to activate the product key, you get a message similar to the following example:

> Unable to verify product key
> The specified product key is invalid, or is unsupported by this version of VAMT. An update to support additional products may be available online.

Possible causes

There may be a problem in the `pkconfig` files. Those files may have to be replaced.

Actions to take

To update the VAMT configuration files, follow these steps:

1. Download the VAMT files.

   The download includes the following files:

   - pkconfig_win7.xrm-ms
   - pkconfig_vista.xrm-ms

2. Copy the two downloaded files into C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\VAMT3\pkconfig, replacing the older versions of the files.

3. Close VAMT, and then restart it.

Unable to connect to the WMI service on the remote machine while activating the remote machine using VAMT online/proxy activation

When you try to activate the product key, you receive a message similar to the following example:

> Unable to connect to the WMI service on the remote machine while activating the remote machine using VAMT online/proxy activation.

Possible causes

Either of the following conditions on the affected computer may cause this problem:

- The WMI (Windows Management Instrumentation) service isn't turned on.
- Windows Firewall isn't configured correctly to allow VAMT access.

Actions to take

- To turn on the WMI service, select **Start** > **Services**, and right-click **Windows Management Instrumentation**. Then select **Restart**.
- To configure Windows Firewall, follow the instructions in Configure Client Computers.

For more information about how to install the VAMT tool and configure client computers, see Install and Configure VAMT.

Error: Access is denied

When you try to activate the product key, you receive a message similar to the following example:

> Error: Access is denied.

Possible Cause

You don't have permissions to access the computer.

Actions to take

On a domain-joined VAMT client computer, verify that:

1. You (or the activating user) have permissions to access the client computer.
2. Your account (or that of the activating user) appears in the **User Accounts** list on the client computer. For more information, see Local Accounts.

Phone activation

This section describes problems that you might experience when you use phone activation.

Error: 0xC004F04D The Software Licensing Service determined that the Installation ID (IID) or the Confirmation ID (CID) is invalid

When you try to activate the product key, you receive a message similar to the following example:

> Run 'slui.exe 0x2a 0xC004F04D' to display the error text.
> Error: 0xC004F04D

Possible Cause

The confirmation ID is incorrect.

Actions to take

1. Call the Microsoft Licensing Activation Centers again. They'll walk you through the steps to get a confirmation ID.
2. In an elevated Command Prompt window, run the following command: `slmgr /atp <Confirmation ID> <ESU Activation ID>`.

> **Note**
>
> In this command, <Confirmation ID> represents the confirmation ID that you obtained in step 1, and <ESU Activation ID> represents the activation ID of the ESU product key.

Installing ESU

You may experience the following problems when you install an ESU update on a computer. This section assumes that the computer has all of the prerequisite updates for

ESU, and the product activation key is installed and activated.

The Windows Module Installer must be updated before you can install the package

When you install an ESU update, you see a message similar to the following example:

> Windows Update Standalone Installer
> The Windows Modules Installer must be updated before you can install this package. Please update the Windows Modules Installer on your computer, then retry Setup.

Possible cause

The Servicing Stack Update (SSU) with AI Changes package isn't installed on the computer.

Actions to take

Verify that the SSU package is installed on the computer. To do so, on the affected computer, select **Start** > **Control Panel** > **Programs** > **Program and Features** > **View Installed updates**.

If the SSU package isn't installed, install it and restart the computer. For more information about this update, see the "Installation prerequisites" section of Obtaining Extended Security Updates for eligible Windows devices.

Additional steps

If the preceding steps don't resolve the problem, on the affected computer, copy the component-based servicing (CBS) log file (C:\Windows\Logs\CBS\CBS.log). Contact Microsoft Support, and provide this log file.

Some updates weren't installed while trying to install the security update

When you install an ESU update, you see a message similar to the following example:

> Download and Install Updates Some updates were not installed For information about other error codes, refer to the Windows Update error reference.

Possible causes

This problem may occur under any of the following conditions:

- A valid ESU key isn't installed on the computer.
- On a desktop client or server, the ESU key is installed but isn't activated.
- On a Windows Embedded device, see Windows Embedded devices for possible causes.
- The Windows operating system that is installed on the computer isn't in the list of ESU supported editions or architectures. For a list of the supported editions and architectures, see Obtaining Extended Security Updates for eligible Windows devices.

Actions to take

On a desktop client or server computer, follow these steps to verify that the computer has a valid ESU key installed and activated.

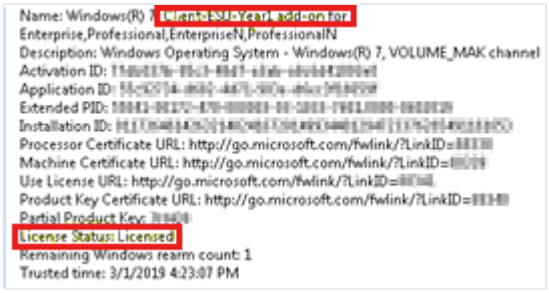
1. Open an elevated Command Prompt window and then run one of the following commands:

   - `slmgr /dlv` (Windows 7 only)
   - `slmgr /dlv <Activation ID>`

     > **Note**
     >
     > In this command, **<Activation ID>** represents the activation ID of the ESU key that is installed on the computer.

   - `slmgr /dlv all`

2. In the command output, verify that ESU key is licensed.

   On a typical (non-embedded) computer, install the ESU key if you haven't already done so. Then activate the key by using one of the following methods:

- VAMT online or proxy activation
- Phone activation
- By using the `slmgr /ato` command. To do so, follow these steps:
  a. Open an elevated Command Prompt window.
  b. Run `slmgr /ipk <ESU key>` and wait for the success message.

> **Note**
>
> In this command, **<ESU key>** represents the ESU product key for the computer.

3. Run `slmgr /ato <Activation ID>`.

On a Windows Embedded device, see Windows Embedded devices for appropriate actions to take.

Additional steps

If the preceding steps don't resolve the problem, on the affected computer, copy the component-based servicing (CBS) log file (C:\Windows\Logs\CBS\CBS.log). Contact Microsoft Support, and provide this log file.

Error: 80070643 - prep-check KB installation fails

When you install an ESU update, you see a message similar to the following example:

> Error: 80070643 - prep-check KB installation fails

The message may reference one of the following KBs:

- KB 4528081 for Windows Server 2008 SP2
- KB 4528069 for Windows 7 / Windows Server 2008R2

The CBS log may contain messages similar to the following example:

- ESU: Product = 36 (0x00000024).
- ESU: Is IMDS check needed: FALSE
- ESU: Pre IMDS checks failed, Not Eligible:HRESULT_FROM_WIN32(1605)
- 1605 = ERROR_UNKNOWN_PRODUCT

Possible causes

- The operating system edition is not supported by the prep-check KB. The prep-check KB doesn't support `*V` or `*Core` editions.
- The most recent Servicing Stack Update (February 11, 2020, or later) and Monthly Rollup update (February 11, 2020, or later) aren't installed on the computer.

Actions to take

Install the latest Servicing Stack Update (February 11, 2020, or later) and Monthly Rollup (February 11, 2020, or later), and then try again.

Windows Embedded devices

When you install ESU on a device that runs a Windows Embedded operating system, you may notice the following problems. ESU: NO ESU KEY FOUND

You have a device with a Windows product key that falls within the range of keys defined for embedded editions of Windows. When you install an ESU update, some of the updates don't install. And the CBS log contains entries similar to the following example:

Output

```
ESU: NO ESU KEY FOUND
```

For example, you see the following log entries.

```
2020-01-17 02:17:04, Info                  CSI    00000001 ESU: Product = 48 (0x00000030).
2020-01-17 02:17:04, Info                  CSI    00000002 ESU: checking : 33 (0x00000021)
2020-01-17 02:17:04, Info                  CSI    00000003 ESU: Product is in Range
2020-01-17 02:17:04, Info                  CSI    00000004 ESU: NO ESU KEY FOUND
2020-01-17 02:17:04, Info                  CSI    00000005 ESU: checking : 33 (0x00000021)
2020-01-17 02:17:04, Info                  CSI    00000006 ESU: Product is in Range
2020-01-17 02:17:04, Info                  CSI    00000007 ESU: NO ESU KEY FOUND
2020-01-17 02:17:04, Info                  CSI    00000008 ESU: checking : 33 (0x00000021)
2020-01-17 02:17:04, Info                  CSI    00000009 ESU: Product is in Range
2020-01-17 02:17:04, Info                  CSI    0000000a ESU: NO ESU KEY FOUND
2020-01-17 02:17:04, Info                  CSI    0000000b ESU: Is IMDS check needed:TRUE
2020-01-17 02:17:04, Info                  CSI    0000000c ESU: Checking IMDS
2020-01-17 02:17:04, Info                  CSI    0000000d ESU: not eligible HRESULT_FROM_WIN32(1633).
```

Possible cause

The ESU product key isn't installed on the device.

Actions to take

Install a valid Windows Embedded ESU key on the computer, and then try to install the ESU package again.

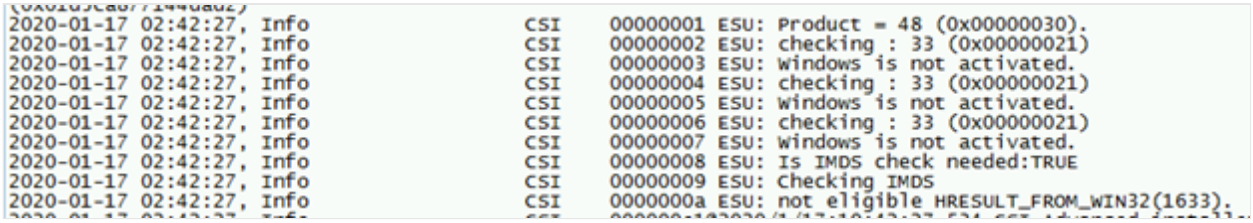
HRESULT_FROM_WIN32(1633), Windows key in range of Windows Embedded keys

You have a device that has a Windows product key that falls within the range of keys that has been defined for embedded editions of Windows. When you install an ESU update, some of the updates don't install, and the CBS log contains entries similar to the following example:

Output

```
ESU: Windows is not activated.
ESU: not eligible:HRESULT_FROM_WIN32(1633)
```

For example, you see the following log entries.



Possible cause

Either the Windows product key or the ESU product key (or both) is installed on the device but isn't activated.

Actions to take

Activate the Windows product key or the ESU product key (or both) and try to install the ESU package.

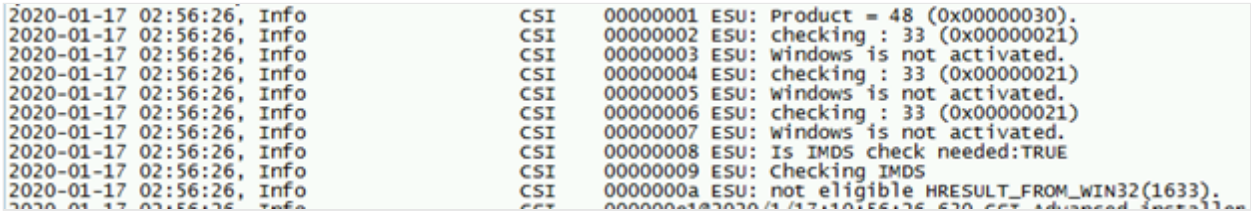
HRESULT_FROM_WIN32(1633), Windows key out of range of Windows Embedded keys

You have a device with a Windows product key that doesn't fall within the range of keys defined for embedded editions of Windows. When you install an ESU update, some of the updates don't install and the CBS log contains entries similar to the following example:

Output

```
ESU: Windows is not activated.
ESU: not eligible:HRESULT_FROM_WIN32(1633)
```

For example, you see the following log entries.



Possible cause

The ESU product key is installed on the computer but isn't activated.

Actions to take

Activate the ESU product key, and then try to install the ESU package again.

Maintaining ongoing ESU compliance

You notice a non-compliant device in your update management and compliance toolsets.

If you have a subset of devices that are running Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1 without ESU, you notice a non-compliant device in your update management and compliance toolsets.

Windows Server Update Service (WSUS) continues to scan cab files for Windows 7 SP1 and Windows Server 2008 R2 SP1.

More information

- Troubleshooting Windows volume activation
- Resolve Windows activation error codes
- Using the Activation troubleshooter
- Get help with Windows activation errors
- FAQ about Extended Security Updates for Windows 7
- Obtaining Extended Security Updates for eligible Windows devices
- How to use Windows Server 2008 and 2008 R2 extended security updates (ESU)

- Extended Security Updates and Configuration Manager
- What are Extended Security Updates for SQL Server?
- Lifecycle FAQ-Extended Security Updates

Windows Security troubleshooting documentation for Windows clients

Article • 06/17/2021 • 2 minutes to read

The topics in this section provide solutions and scenario guides to help you troubleshoot and self-solve Windows Security-related issues. The topics are divided into subcategories. Browse the content or use the search feature to find relevant content.

Windows Security sub categories

- Account lockouts
- Bitlocker
- Kerberos authentication
- Legacy authentication (NTLM)
- Permissions, access control, and auditing
- Secure Boot and UEFI
- Smart card logon
- TPM
- Windows Firewall with Advanced Security (WFAS)

How to access the computer after you disable the administrator account

Article • 09/23/2021 • 2 minutes to read

This article describes how to access your Microsoft Windows Server 2003-based computer by using the Administrator account after you disable the local Administrator account.

Applies to: Windows Server 2003
Original KB number: 814777

Summary

You can use Windows Server 2003 to disable the local Administrator account. This feature is included to provide an additional level of security in your organization. Additionally, the default Remote Installation Services (RIS) installation disables the local Administrator account on the destination computer.

Log on to Windows by using Safe mode

To log on to Windows by using the disabled local Administrator account, start Windows in Safe mode. Even when the Administrator account is disabled, you are not prevented from logging on as Administrator in Safe mode. When you have logged on successfully in Safe mode, re-enable the Administrator account, and then log on again. To do this, follow these steps:

1. Start the computer, and then press the F8 key when the Power On Self Test (POST) is complete.
2. From the **Windows Advanced Options** menu, use the ARROW keys to select **Safe Mode**, and then press ENTER.
3. Select the operating system that you want to start, and then press ENTER.
4. Log on to Windows as Administrator. If you are prompted to do so, click to select an item in the **Why did the computer shut down unexpectedly** list, and then click **OK**.
5. On the message that states Windows is running in safe mode, click **OK**.
6. Click **Start**, right-click **My Computer**, and then click **Manage**.
7. Expand **Local Users and Groups**, click **Users**, right-click **Administrator** in the right pane, and then click **Properties**.
8. Click to clear the **Account is disabled** check box, and then click **OK**.

If the server is a domain controller, the Local Users and Groups are not available in **Computer Management**. To enable the Administrator account, follow these steps:

1. Start your computer to Safe mode with networking support.
2. Log on as the administrator.
3. Click **Start**, click **Run**, type *cmd*, and then press Enter.
4. At the command prompt, type the following command, and then press Enter:

```
Console

net user administrator /active:yes
```

Log on to Windows by using Recovery Console

You can use the recovery console to access the computer even if the local Administrator account is disabled. Disabling the local Administrator account does not prevent you from logging on to the recovery console as Administrator.

Decode Measured Boot logs to track PCR changes

Article • 11/23/2022 • 3 minutes to read

Platform Configuration Registers (PCRs) are memory locations in the Trusted Platform Module (TPM). BitLocker and its related technologies depend on specific PCR configurations. Additionally, specific change in PCRs can cause a device or computer to enter BitLocker recovery mode.

By tracking changes in the PCRs, and identifying when they changed, insight can be gained into issues that occur or learn why a device or computer entered BitLocker recovery mode. The Measured Boot logs record PCR changes and other information. These logs are located in the *C:\Windows\Logs\MeasuredBoot* folder.

This article describes tools that can be used to decode these logs:

- TBSLogGenerator.exe
- PCPTool.exe

For more information about Measured Boot and PCRs, see the following articles:

- TPM fundamentals: Measured Boot with support for attestation
- Understanding PCR banks on TPM 2.0 devices

Use TBSLogGenerator.exe to decode Measured Boot logs

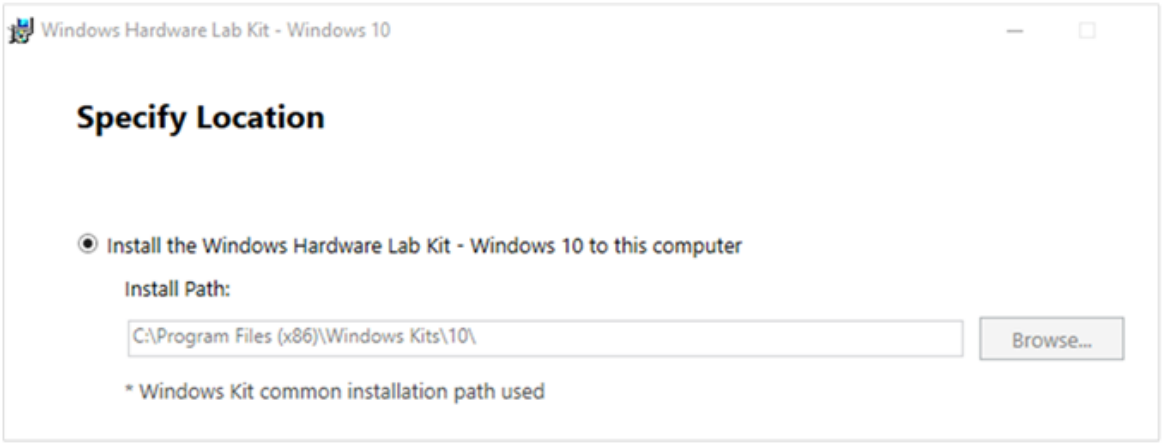
Use *TBSLogGenerator.exe* to decode Measured Boot logs that were collected from Windows. *TBSLogGenerator.exe* can be installed on the following systems:

- A computer that is running Windows Server 2016 or newer and that has a TPM enabled
- A Gen 2 virtual machine running on Hyper-V that is running Windows Server 2016 or newer and is using a virtual TPM.

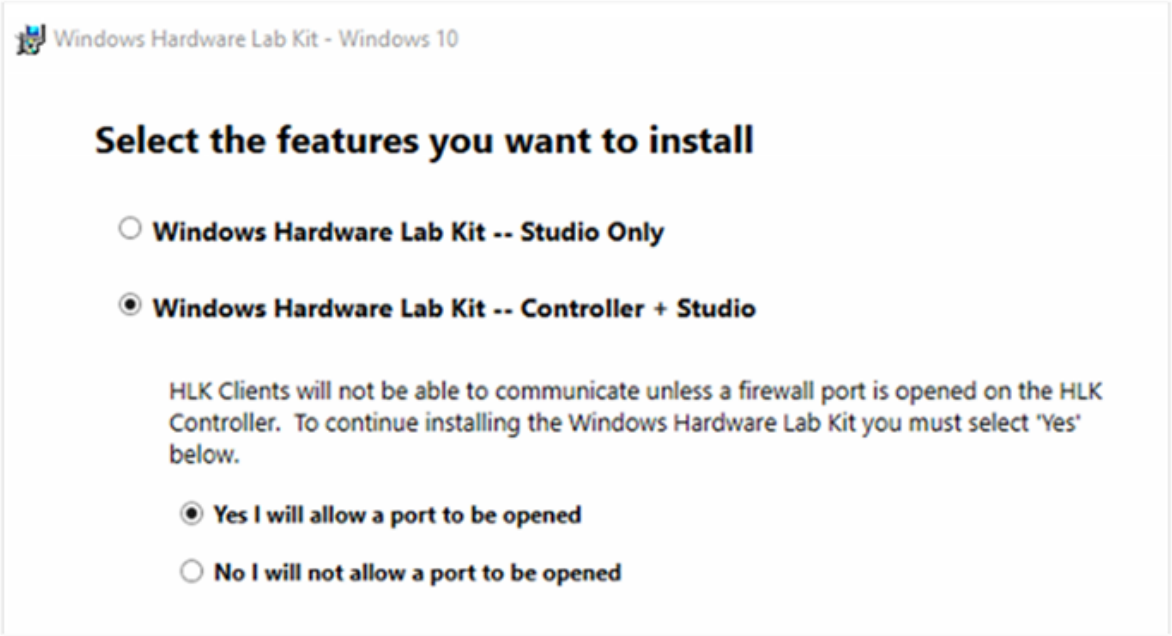
To install the tool, follow these steps:

1. Download the Windows Hardware Lab Kit from Windows Hardware Lab Kit.
2. After downloading, run the installation file from the path where the install was downloaded to.

3. Accept the default installation path.



4. Under **Select the features you want to install**, select **Windows Hardware Lab Kit—Controller + Studio**.



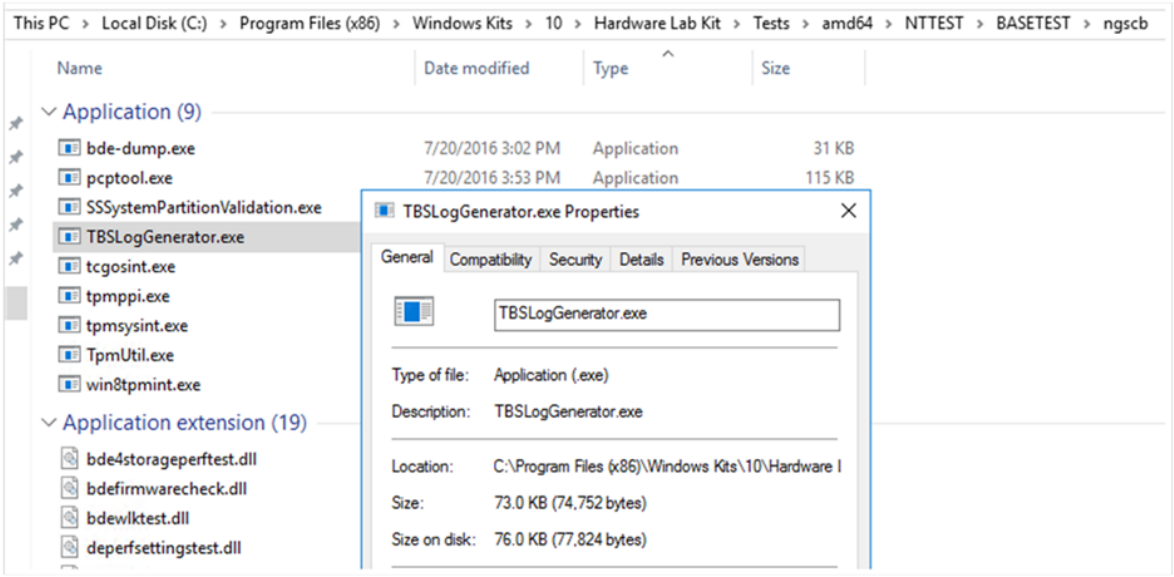
5. Finish the installation.

To use *TBSLogGenerator.exe*, follow these steps:

1. After the installation finishes, open an elevated Command Prompt window and navigate to the following folder:

   C:\Program Files (x86)\Windows Kits\10\Hardware Lab Kit\Tests\amd64\NTTEST\BASETEST\ngscb

   This folder contains the *TBSLogGenerator.exe* file.



2. Run the following command:

```
cmd

TBSLogGenerator.exe -LF <LogFolderName>\<LogFileName>.log >
<DestinationFolderName>\<DecodedFileName>.txt
```

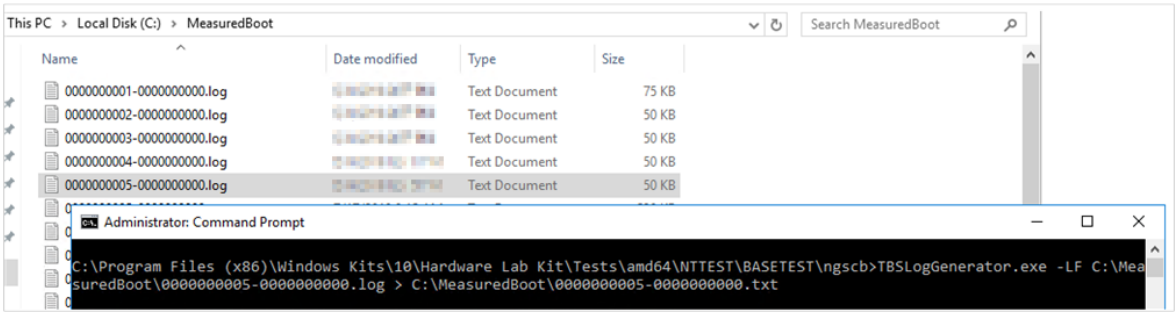
where the variables represent the following values:

- *<LogFolderName>* = the name of the folder that contains the file to be decoded
- *<LogFileName>* = the name of the file to be decoded
- *<DestinationFolderName>* = the name of the folder for the decoded text file
- *<DecodedFileName>* = the name of the decoded text file

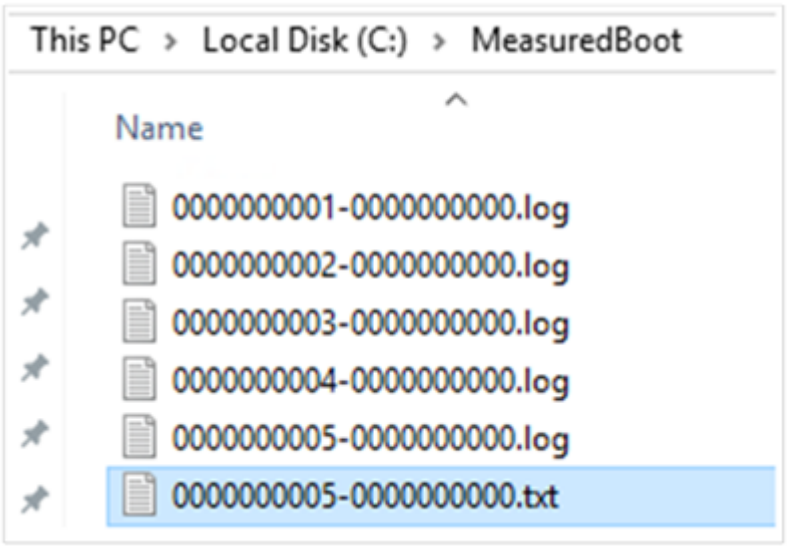
For example, the following figure shows Measured Boot logs that were collected from a Windows 10 computer and put into the *C:\MeasuredBoot* folder. The figure also shows a Command Prompt window and the command to decode the *0000000005-0000000000.log* file:

```
cmd

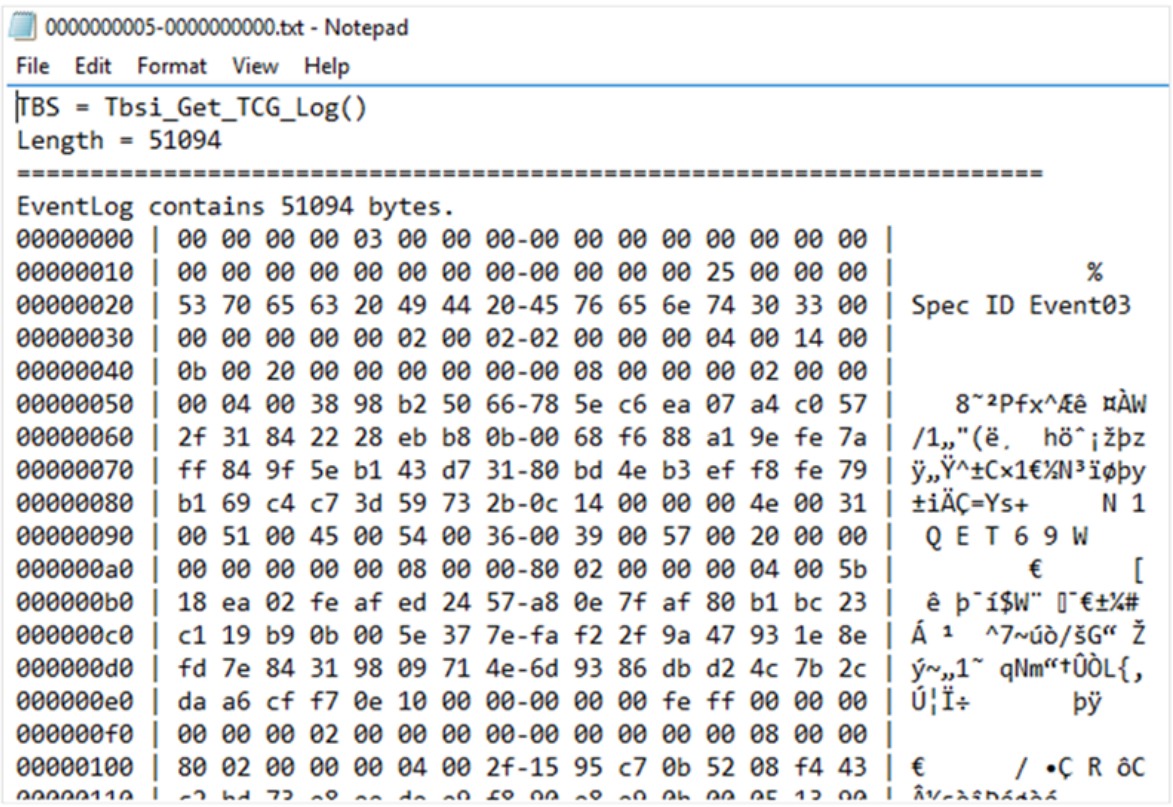
TBSLogGenerator.exe -LF C:\MeasuredBoot\0000000005-0000000000.log >
C:\MeasuredBoot\0000000005-0000000000.txt
```



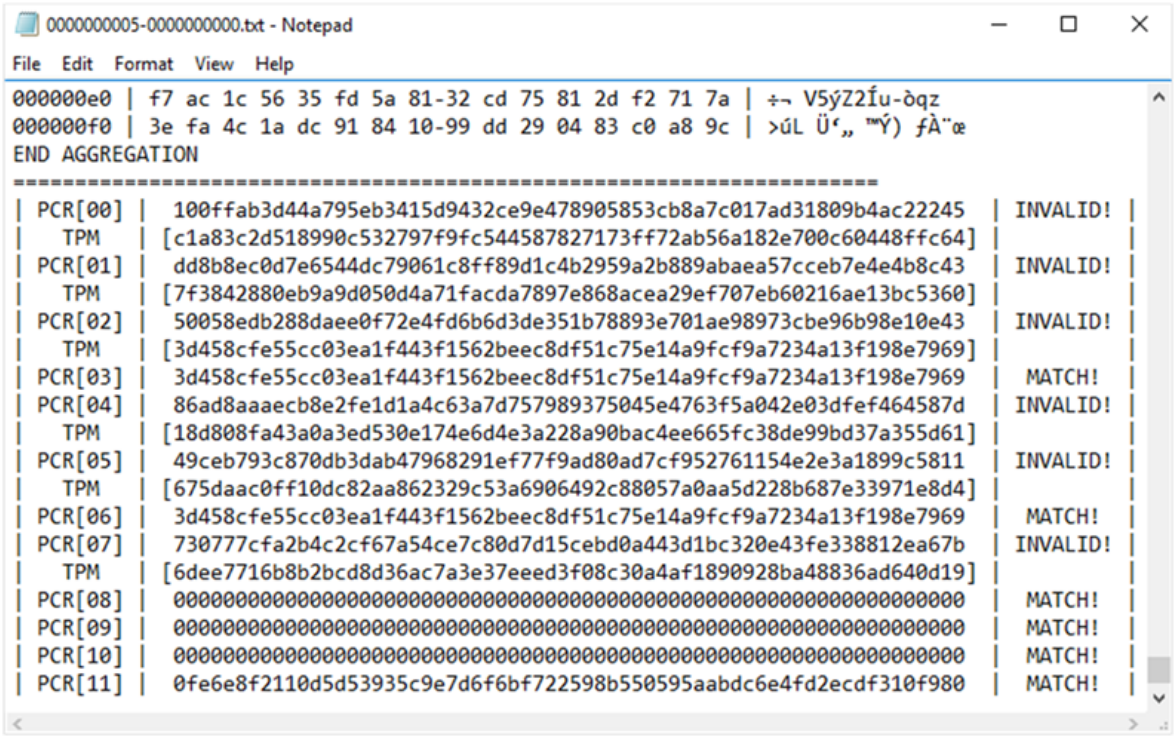
The command produces a text file that uses the specified name. In this example, the file is *0000000005-0000000000.txt*. The file is located in the same folder as the original *.log* file.



The content of this text file is similar to the following text:



To find the PCR information, go to the end of the file.



Use PCPTool.exe to decode Measured Boot logs

> **Note**
>
> *PCPTool.exe* is a Visual Studio solution, but executable needs to be built before tool can be used.

PCPTool.exe is part of the TPM Platform Crypto-Provider Toolkit. The tool decodes a Measured Boot log file and converts it into an XML file.

To download and install *PCPTool.exe*, go to the Toolkit page, select **Download**, and follow the instructions.

To decode a log, run the following command:

```cmd
PCPTool.exe decodelog <LogFolderPath>\<LogFileName>.log >
<DestinationFolderName>\<DecodedFileName>.xml
```

where the variables represent the following values:

- *<LogFolderPath>* = the path to the folder that contains the file to be decoded

- <*LogFileName*> = the name of the file to be decoded
- <*DestinationFolderName*> = the name of the folder for the decoded text file
- <*DecodedFileName*> = the name of the decoded text file

The content of the XML file will be similar to the following XML:

```
> .\PCPTool.exe decodelog C:\Windows\Logs\MeasuredBoot\0000000001-0000000000.log > TPM_log.xml
```

```
129      </EV_Event_Tag>
130      <EV_Event_Tag PCR="13" EventDigest="3db51a2ab6859f67510849226e545d7a193b66eb" Size="760">
131        <Trustboundary Size="752">
132          <SipaEvent Type="0x00040002" Size="46">
133            00ad31d5660ed001200000000b00f4247831deed0fc371f8e8a6b0746ae7b508c3c924e5b1c485c14631afa33879
134            <!-- ..1.f..........x1....q....tj..........F1..8y -->
135          </SipaEvent>
136          <LoadedModule_Aggregation Size="354">
137            <FilePath Size="86">\EFI\Microsoft\Boot\en-GB\bootmgfw.efi.MUI</FilePath>
138            <ImageSize Size="8">69632<!-- 0x0000000000011000 --></ImageSize>
139            <HashAlgorithmId Size="4">SHA-256</HashAlgorithmId>
140            <AuthenticodeHash Size="32">
141              a1cd73aee5d6f2c87e57573f0e50b8ab7f512dcf7c544df8ae231d492d5835b8
142              <!-- ..s......WW..P...Q...TM....I.X5. -->
143            </AuthenticodeHash>
144            <ImageValidated Size="1">TRUE</ImageValidated>
145            <AuthorityIssuer Size="76">Microsoft Windows Production PCA 2011</AuthorityIssuer>
146            <AuthorityPublisher Size="36">Microsoft Windows</AuthorityPublisher>
```

BitLocker and TPM: other known issues

Article • 11/23/2022 • 5 minutes to read

This article describes common issues that relate directly to the trusted platform module (TPM), and provides guidance to address these issues.

Azure AD: Windows Hello for Business and single sign-on don't work

Consider the following scenario:

An Azure Active Directory (Azure AD)-joined client computer can't authenticate correctly. The computer is experiencing one or more of the following symptoms:

- Windows Hello for Business doesn't work
- Conditional access fails
- Single sign-on (SSO) doesn't work

Additionally, in Event Viewer, the computer logs the following Event ID 1026 event under **Windows Logs** > **System**:

> Log Name: System
> Source: Microsoft-Windows-TPM-WMI
> Date: <Date and Time>
> Event ID: 1026
> Task Category: None
> Level: Information
> Keywords:
> User: SYSTEM
> Computer: <Computer name>
> Description:
> The Trusted Platform Module (TPM) hardware on this computer cannot be provisioned for use automatically. To set up the TPM interactively use the TPM management console (Start->tpm.msc) and use the action to make the TPM ready.
> Error: The TPM is defending against dictionary attacks and is in a time-out period.
> Additional Information: 0x840000

Cause of Azure AD: Windows Hello for Business and single sign-on don't work

This event indicates that the TPM isn't ready or has some setting that prevents access to the TPM keys.

Additionally, the behavior indicates that the client computer can't obtain a Primary Refresh Token (PRT).

Resolution for Azure AD: Windows Hello for Business and single sign-on don't work

To verify the status of the PRT, use the dsregcmd.exe /status command to collect information. In the tool output, verify that either **User state** or **SSO state** contains the **AzureAdPrt** attribute. If the value of this attribute is **No**, the PRT wasn't issued. If the value of the attribute is **No**, it may indicate that the computer couldn't present its certificate for authentication.

To resolve this issue, follow these steps to troubleshoot the TPM:

1. Open the TPM management console (*tpm.msc*) by selecting **Start** and entering **tpm.msc** in the **Search** box.
2. If a notice is displayed to either unlock the TPM or reset the lockout, contact the hardware vendor to determine whether there's a known fix for the issue.
3. If the issue is still not resolved after contacting the hardware vendor, clear and reinitialize the TPM by following the instructions in the article Troubleshoot the TPM: Clear all the keys from the TPM.

   > ⚠ **Warning**
   >
   > Clearing the TPM can cause data loss.

If in Step 2 there's no notice to either unlock the TPM or reset the lockout, review the UEFI firmware/BIOS settings of the computer for any setting that can be used to reset or disable the lockout.

TPM 1.2 Error: Loading the management console failed. The device that is required by the cryptographic provider isn't ready for use

Consider the following scenario:

When trying to open the TPM management console on a Windows computer that uses TPM version 1.2, the following message is displayed:

> Loading the management console failed. The device that is required by the cryptographic provider is not ready for use.
> HRESULT 0x800900300x80090030 - NTE_DEVICE_NOT_READY
> The device that is required by this cryptographic provider is not ready for use.
> TPM Spec version: TPM v1.2

On a different device that is running the same version of Windows, the TPM management console can be opened.

Cause (suspected) of TPM 1.2 Error: Loading the management console failed. The device that is required by the cryptographic provider isn't ready for use

These symptoms indicate that the TPM has hardware or firmware issues.

Resolution for TPM 1.2 Error: Loading the management console failed. The device that is required by the cryptographic provider isn't ready for use

To resolve the issue:

- Switch the TPM operating mode from version 1.2 to version 2.0 if the device has this option available.
- If switching the TPM from version 1.2 to version 2.0 doesn't resolve the issue, or if the device doesn't have TPM version 2.0 available, contact the hardware vendor to determine whether there's a UEFI firmware update/BIOS update/TPM update for the device. If there's an update available, install the update to see if it resolves the issue.
- If updating the UEFI firmware/BIOS doesn't resolve the issue, or if there's no update available, consider replacing the device motherboard by contacting the hardware vendor. After the motherboard has been replaced, switch the TPM operating mode from version 1.2 to version 2.0 if this option is available.

  > ⚠ **Warning**
  >
  > Replacing the motherboard will cause data in the TPM to be lost.

Devices don't join hybrid Azure AD because of a TPM issue

When trying to join a device to a hybrid Azure AD, the join operation appears to fail.

To verify that the join succeeded, use the dsregcmd /status command. In the tool output, the following attributes indicate that the join succeeded:

- **AzureAdJoined: YES**
- **DomainName: <*on-prem Domain name*>**

If the value of **AzureADJoined** is **No**, the join operation failed.

Causes and resolutions for devices don't join hybrid Azure AD because of a TPM issue

This issue may occur when the Windows operating system isn't the owner of the TPM. The specific fix for this issue depends on which errors or events are displayed, as shown in the following table:

Message	Reason	Resolution
NTE_BAD_KEYSET (0x80090016/-2146893802)	TPM operation failed or was invalid	This issue was probably caused by a corrupted sysprep image. When creating a sysprep image, make sure to use a computer that isn't joined to or registered in Azure AD or hybrid Azure AD.
TPM_E_PCP_INTERNAL_ERROR (0x80290407/-2144795641)	Generic TPM error.	If the device returns this error, disable its TPM. Windows 10, version 1809 and later versions, automatically detect TPM failures and finish the hybrid Azure AD join without using the TPM.
TPM_E_NOTFIPS (0x80280036/-2144862154)	The FIPS mode of the TPM is currently not supported.	If the device gives this error, disable its TPM. Windows 10, version 1809 and later versions, automatically detect TPM failures and finish the hybrid Azure AD join without using the TPM.
NTE_AUTHENTICATION_IGNORED (0x80090031/-2146893775)	The TPM is locked out.	This error is transient. Wait for the cooldown period, and then retry the join operation.

For more information about TPM issues, see the following articles:

- TPM fundamentals: Anti-hammering
- Troubleshooting hybrid Azure Active Directory-joined devices
- Troubleshoot the TPM

BitLocker cannot encrypt a drive: known TPM issues

Article • 11/23/2022 • 5 minutes to read

This article describes common issues that affect the Trusted Platform Module (TPM) that might prevent BitLocker from encrypting a drive. This article also provides guidance to address these issues.

> ⓘ Note
>
> If it's been determined that the BitLocker issue does not involve the TPM, see **BitLocker cannot encrypt a drive: known issues**.

The TPM is locked and the error `The TPM is defending against dictionary attacks and is in a time-out period` is displayed

It's attempted to turn on BitLocker drive encryption on a device but it fails with an error message similar to the following error message:

> **The TPM is defending against dictionary attacks and is in a time-out period.**

Cause of the TPM being locked

The TPM is locked out.

Resolution for the TPM being locked

To resolve this issue, the TPM needs to be reset and cleared. The TPM can be reset and cleared with the following steps:

1. Open an elevated PowerShell window and run the following script:

```PowerShell
$Tpm = Get-WmiObject -class Win32_Tpm -namespace
"root\CIMv2\Security\MicrosoftTpm"
$ConfirmationStatus =
```

```
$Tpm.GetPhysicalPresenceConfirmationStatus(22).ConfirmationStatus
if($ConfirmationStatus -ne 4) {$Tpm.SetPhysicalPresenceRequest(22)}
```

2. Restart the computer. If a prompt is displayed confirming the clearing of the TPM, agree to clear the TPM.

3. Sign on to Windows and retry starting BitLocker drive encryption.

> ⚠ **Warning**
>
> Resetting and clearing the TPM can cause data loss.

The TPM fails to prepare with the error `The TPM is defending against dictionary attacks and is in a time-out period`

It's attempted to turn on BitLocker drive encryption on a device but it fails. While troubleshooting, the TPM management console (*tpm.msc*) is used to attempt to prepare the TPM on the device. The operation fails with an error message similar to the following error message:

> The TPM is defending against dictionary attacks and is in a time-out period.

Cause of TPM failing to prepare

The TPM is locked out.

Resolution for TPM failing to prepare

To resolve this issue, disable and re-enable the TPM with the following steps:

1. Enter the UEFI/BIOS configuration screens of the device by restarting the device and hitting the appropriate key combination as the device boots. Consult with the device manufacturer for the appropriate key combination for entering into the UEFI/BIOS configuration screens.

2. Once in the UEFI/BIOS configuration screens, disable the TPM. Consult with the device manufacturer for instructions on how to disable the TPM in the UEFI/BIOS configuration screens.

3. Save the UEFI/BIOS configuration with the TPM disabled and restart the device to boot into Windows.
4. Once signed into Windows, return to the TPM management console. An error message similar to the following error message is displayed:

   > Compatible TPM cannot be found
   >
   > Compatible Trusted Platform Module (TPM) cannot be found on this computer. Verify that this computer has 1.2 TPM and it is turned on in the BIOS.

   This message is expected since the TPM is currently disabled in the UEFI firmware/BIOS of the device.
5. Restart the device and enter the UEFI/BIOS configuration screens again.
6. Reenable the TPM in the UEFI/BIOS configuration screens.
7. Save the UEFI/BIOS configuration with the TPM enabled and restart the device to boot into Windows.
8. Once signed into Windows, return to the TPM management console.

If the TPM still can't be prepared, clear the existing TPM keys by following the instructions in the article Troubleshoot the TPM: Clear all the keys from the TPM.

> ⚠ **Warning**
>
> Clearing the TPM can cause data loss.

BitLocker fails to enable with the error `Access Denied: Failed to backup TPM Owner Authorization information to Active Directory Domain Services. Errorcode: 0x80070005` or `Insufficient Rights`

The **Do not enable BitLocker until recovery information is stored in AD DS** policy is enforced in the environment. It's attempted to turn on BitLocker drive encryption on a device but it fails with the error message of `Access Denied: Failed to backup TPM Owner`

`Authorization information to Active Directory Domain Services. Errorcode: 0x80070005` or `Insufficient Rights`.

Cause of `Access Denied` or `Insufficient Rights`

The TPM didn't have sufficient permissions on the TPM devices container in Active Directory Domain Services (AD DS). Therefore, the BitLocker recovery information couldn't be backed up to AD DS, and BitLocker drive encryption couldn't turn on.

This issue appears to be limited to computers that run versions of Windows that are earlier than Windows 10.

Resolution for `Access Denied` or `Insufficient Rights`

To verify this issue is occurring, use one of the following two methods:

- Disable the policy or remove the computer from the domain followed by trying to turn on BitLocker drive encryption again. If the operation succeeds, then the issue was caused by the policy.
- Use LDAP and network trace tools to examine the LDAP exchanges between the client and the AD DS domain controller to identify the cause of the **Access Denied** or **Insufficient Rights** error. In this case, an error should be displayed when the client tries to access its object in the `CN=TPM Devices,DC=<domain>,DC=com` container.

1. To review the TPM information for the affected computer, open an elevated Windows PowerShell window and run the following command:

   ```
   PowerShell

   Get-ADComputer -Filter {Name -like "ComputerName"} -Property * |
   Format-Table name,msTPM-TPMInformationForComputer
   ```

   In this command, *ComputerName* is the name of the affected computer.

2. To resolve the issue, use a tool such as *dsacls.exe* to ensure that the access control list of msTPM-TPMInformationForComputer grants both **Read** and **Write** permissions to **NTAUTHORITY/SELF**.

The TPM fails to be prepared with the error `0x80072030: There is no such object on the`

server

Domain controllers were upgraded from Windows Server 2008 R2 to Windows Server 2012 R2. A group policy object (GPO) exists that enforces the **Do not enable BitLocker until recovery information is stored in AD DS** policy.

It's attempted to turn on BitLocker drive encryption on a device but it fails. While troubleshooting, the TPM management console (*tpm.msc*) is used to attempt to prepare the TPM on the device. The operation fails with an error message similar to the following error message:

> 0x80072030 There is no such object on the server when a policy to back up TPM information to active directory is enabled

It's been confirmed that the **ms-TPM-OwnerInformation** and **msTPM-TpmInformationForComputer** attributes are present.

Cause of 0x80072030: There is no such object on the server

The domain and forest functional level of the environment may still be set to Windows 2008 R2. Additionally, the permissions in AD DS might not be correctly set.

Resolution for 0x80072030: There is no such object on the server

The issue can be resolved with the following steps:

1. Upgrade the functional level of the domain and forest to Windows Server 2012 R2.
2. Download Add-TPMSelfWriteACE.vbs.
3. In the script, modify the value of **strPathToDomain** to the organization's domain name.
4. Open an elevated PowerShell window, and run the following command:

   ```
   cmd
   ```

   ```
   cscript.exe <Path>\Add-TPMSelfWriteACE.vbs
   ```

   In this command, <*Path*> is the path to the script file.

For more information, see the following articles:

- Back up the TPM recovery information to AD DS
- Prepare your organization for BitLocker: Planning and policies

BitLocker configuration: known issues

Article • 11/23/2022 • 6 minutes to read

This article describes common issues that affect BitLocker's configuration and general functionality. This article also provides guidance to address these issues.

BitLocker encryption is slower in Windows 10 and Windows 11

BitLocker runs in the background to encrypt drives. However, in Windows 11 and Windows 10, BitLocker is less aggressive about requesting resources than in previous versions of Windows. This behavior reduces the chance that BitLocker will affect the computer's performance.

To compensate for these changes, BitLocker uses a conversion model called Encrypt-On-Write. This model makes sure that any new disk writes are encrypted as soon as BitLocker is enabled. This behavior happens on all client editions and for any internal drives.

> **Important**
>
> To preserve backward compatibility, BitLocker uses the previous conversion model to encrypt removable drives.

Benefits of using the new conversion model

By using the previous conversion model, an internal drive can't be considered protected and compliant with data protection standards until the BitLocker conversion is 100 percent complete. Before the process finishes, the data that existed on the drive before encryption began - that is, potentially compromised data - can still be read and written without encryption. Therefore, for data to be considered protected and compliant with data protection standards, the encryption process has to finish before sensitive data is stored on the drive. Depending on the size of the drive, this delay can be substantial.

By using the new conversion model, sensitive data can be stored on the drive as soon as BitLocker is turned on. The encryption process doesn't need to finish first, and encryption doesn't adversely affect performance. The tradeoff is that the encryption process for pre-existing data takes more time.

Other BitLocker enhancements

Several other areas of BitLocker were improved in versions of Windows released after Windows 7:

- **New encryption algorithm, XTS-AES** - Added in Windows 10 version 1511, this algorithm provides additional protection from a class of attacks on encrypted data that rely on manipulating cipher text to cause predictable changes in plain text.

  By default, this algorithm complies with the Federal Information Processing Standards (FIPS). FIPS is a United States Government standard that provides a benchmark for implementing cryptographic software.

- **Improved administration features**. BitLocker can be managed on PCs or other devices by using the following interfaces:
  - BitLocker Wizard
  - manage-bde.exe
  - Group Policy Objects (GPOs)
  - Mobile Device Management (MDM) policy
  - Windows PowerShell
  - Windows Management Interface (WMI)

- **Integration with Azure Active Directory** (Azure AD) - BitLocker can store recovery information in Azure AD to make it easier to recover.

- Direct memory access (DMA) Port Protection - By using MDM policies to manage BitLocker, a device's DMA ports can be blocked which secures the device during its startup.

- BitLocker Network Unlock - If the BitLocker-enabled desktop or server computer is connected to a wired corporate network in a domain environment, its operating system volume can be automatically unlocked during a system restart.

- **Support for** Encrypted Hard Drives - Encrypted Hard Drives are a new class of hard drives that are self-encrypting at a hardware level and allow for full disk hardware encryption. By taking on that workload, Encrypted Hard Drives increase BitLocker performance and reduce CPU usage and power consumption.

- **Support for classes of HDD/SSD hybrid disks** - BitLocker can encrypt a disk that uses a small SSD as a non-volatile cache in front of the HDD, such as Intel Rapid Storage Technology.

Hyper-V Gen 2 VM: Can't access the volume after BitLocker encryption

Consider the following scenario:

1. BitLocker is turned on a generation 2 virtual machine (VM) that runs on Hyper-V.
2. Data is added to the data disk as it encrypts.
3. The VM is restarted and the following behavior is observed:
    - The system volume isn't encrypted.
    - The encrypted volume isn't accessible, and the computer lists the volume's file system as **Unknown**.
    - A message similar to the following message is displayed:

      > **You need to format the disk in <*drive_letter:*> drive before you can use it**

Cause of not being able to access the volume after BitLocker encryption on a Hyper-V Gen 2 VM

This issue occurs because the third-party filter driver *Stcvsm.sys* (from StorageCraft) is installed on the VM.

Resolution for not being able to access the volume after BitLocker encryption on a Hyper-V Gen 2 VM

To resolve this issue, remove the third-party software.

Production snapshots fail for virtualized domain controllers that use BitLocker-encrypted disks

Consider the following scenario:

A Windows Server 2019 or 2016 Hyper-V Server is hosting VMs (guests) that are configured as Windows domain controllers. On a domain controller guest VM, BitLocker has encrypted the disks that store the Active Directory database and log files. When a

"production snapshot" of the domain controller guest VM is attempted, the Volume Snap-Shot (VSS) service doesn't correctly process the backup.

This issue occurs regardless of any of the following variations in the environment:

- How the domain controller volumes are unlocked.
- Whether the VMs are generation 1 or generation 2.
- Whether the guest operating system is Windows Server 2019, 2016 or 2012 R2.

In the guest VM domain controller **Windows Logs** > **Application** Event Viewer log, the VSS event source records event **ID 8229**:

> ID: 8229
> Level: Warning
> Source: VSS
> Message: A VSS writer has rejected an event with error 0x800423f4. The writer experienced a non-transient error. If the backup process is retried, the error is likely to reoccur.
>
> Changes that the writer made to the writer components while handling the event will not be available to the requester.
>
> Check the event log for related events from the application hosting the VSS writer.
>
> Operation:
> PostSnapshot Event
>
> Context:
> Execution Context: Writer
> Writer Class Id: {b2014c9e-8711-4c5c-a5a9-3cf384484757}
> Writer Name: NTDS
> Writer Instance ID: {d170b355-a523-47ba-a5c8-732244f70e75}
> Command Line: C:\Windows\system32\lsass.exe
>
> Process ID: 680

In the guest VM domain controller **Applications and Services Logs** > **Directory Service** Event Viewer log, there's an event logged similar to the following event:

> Error Microsoft-Windows-ActiveDirectory_DomainService 1168
> Internal Processing Internal error: An Active Directory Domain Services error has occurred.

> Additional Data
> Error value (decimal): -1022
>
> Error value (hex): fffffc02
>
> Internal ID: 160207d9

> **Note**
>
> The internal ID of this event may differ based on the operating system release version and patch level.

When this issue occurs, the **Active Directory Domain Services (NTDS) VSS Writer** will display the following error when the `vssadmin.exe list writers` command is run:

```
Error

Writer name: 'NTDS'
 Writer Id: {b2014c9e-8711-4c5c-a5a9-3cf384484757}
 Writer Instance Id: {08321e53-4032-44dc-9b03-7a1a15ad3eb8}
 State: [11] Failed
 Last error: Non-retryable error
```

Additionally, the VMs can't be backed up until they're restarted.

Cause of production snapshots fail for virtualized domain controllers that use BitLocker-encrypted disks

After VSS creates a snapshot of a volume, the VSS writer takes "post snapshot" actions. When a "production snapshot" is initiated from the host server, Hyper-V tries to mount the snapshotted volume. However, it can't unlock the volume for unencrypted access. BitLocker on the Hyper-V server doesn't recognize the volume. Therefore, the access attempt fails and then the snapshot operation fails.

This behavior is by design.

Workaround for production snapshots fail for virtualized domain controllers that use BitLocker-encrypted disks

A supported way to perform backup and restore of a virtualized domain controller is to run **Windows Server Backup** in the guest operating system.

If a production snapshot of a virtualized domain controller needs to be taken, BitLocker can be suspended in the guest operating system before the production snapshot is started. However, this approach isn't recommended.

For more information and recommendations about backing up virtualized domain controllers, see Virtualizing Domain Controllers using Hyper-V: Backup and Restore Considerations for Virtualized Domain Controllers

More information

When the VSS NTDS writer requests access to the encrypted drive, the Local Security Authority Subsystem Service (LSASS) generates an error entry similar to the following error:

Console

```
\# for hex 0xc0210000 / decimal -1071579136
STATUS\_FVE\_LOCKED\_VOLUME ntstatus.h
\# This volume is locked by BitLocker Drive Encryption.
```

The operation produces the following call stack:

Console

```
\# Child-SP RetAddr Call Site
 00 00000086\`b357a800 00007ffc\`ea6e7a4c KERNELBASE\!FindFirstFileExW+0x1ba
\[d:\\rs1\\minkernel\\kernelbase\\filefind.c @ 872\]
 01 00000086\`b357abd0 00007ffc\`e824accb KERNELBASE\!FindFirstFileW+0x1c \
[d:\\rs1\\minkernel\\kernelbase\\filefind.c @ 208\]
 02 00000086\`b357ac10 00007ffc\`e824afa1 ESENT\!COSFileFind::ErrInit+0x10b
\[d:\\rs1\\onecore\\ds\\esent\\src\\os\\osfs.cxx @ 2476\]
 03 00000086\`b357b700 00007ffc\`e827bf02
ESENT\!COSFileSystem::ErrFileFind+0xa1 \
[d:\\rs1\\onecore\\ds\\esent\\src\\os\\osfs.cxx @ 1443\]
 04 00000086\`b357b960 00007ffc\`e82882a9
ESENT\!JetGetDatabaseFileInfoEx+0xa2 \
[d:\\rs1\\onecore\\ds\\esent\\src\\ese\\jetapi.cxx @ 11503\]
 05 00000086\`b357c260 00007ffc\`e8288166
ESENT\!JetGetDatabaseFileInfoExA+0x59 \
[d:\\rs1\\onecore\\ds\\esent\\src\\ese\\jetapi.cxx @ 11759\]
 06 00000086\`b357c390 00007ffc\`e84c64fb
ESENT\!JetGetDatabaseFileInfoA+0x46 \
[d:\\rs1\\onecore\\ds\\esent\\src\\ese\\jetapi.cxx @ 12076\]
 07 00000086\`b357c3f0 00007ffc\`e84c5f23
ntdsbsrv\!CVssJetWriterLocal::RecoverJetDB+0x12f \
[d:\\rs1\\ds\\ds\\src\\jetback\\snapshot.cxx @ 2009\]
 08 00000086\`b357c710 00007ffc\`e80339e0
ntdsbsrv\!CVssJetWriterLocal::OnPostSnapshot+0x293 \
[d:\\rs1\\ds\\ds\\src\\jetback\\snapshot.cxx @ 2190\]
```

```
 09 00000086\`b357cad0 00007ffc\`e801fe6d
VSSAPI\!CVssIJetWriter::OnPostSnapshot+0x300 \
[d:\\rs1\\base\\stor\\vss\\modules\\jetwriter\\ijetwriter.cpp @ 1704\]
 0a 00000086\`b357ccc0 00007ffc\`e8022193
VSSAPI\!CVssWriterImpl::OnPostSnapshotGuard+0x1d \
[d:\\rs1\\base\\stor\\vss\\modules\\vswriter\\vswrtimp.cpp @ 5228\]
 0b 00000086\`b357ccf0 00007ffc\`e80214f0
VSSAPI\!CVssWriterImpl::PostSnapshotInternal+0xc3b \
[d:\\rs1\\base\\stor\\vss\\modules\\vswriter\\vswrtimp.cpp @ 3552\]
```

BitLocker recovery: known issues

Article • 11/23/2022 • 9 minutes to read

This article describes common issues that may prevent BitLocker from behaving as expected when a drive is recovered, or that may cause BitLocker to start recovery unexpectedly. The article also provides guidance to address these issues.

> **Note**
>
> In this article, "recovery password" refers to the 48-digit recovery password and "recovery key" refers to 32-digit recovery key. For more information, see **BitLocker key protectors**.

Windows prompts for a non-existing BitLocker recovery password

Windows prompts for a BitLocker recovery password. However, a BitLocker recovery password wasn't configured.

Resolution for Windows prompts for a non-existing BitLocker recovery password

The BitLocker and Active Directory Domain Services (AD DS) FAQ address situations that may produce this symptom, and provides information about the procedure to resolve the issue:

- What if BitLocker is enabled on a computer before the computer has joined the domain?
- What happens if the backup initially fails? Will BitLocker retry the backup?

The recovery password for a laptop wasn't backed up, and the laptop is locked

Consider the following scenario:

The hard disk of a Windows 11 or Windows 10 laptop has to be recovered. The disk was encrypted by using BitLocker Driver Encryption. However, the BitLocker recovery

password wasn't backed up, and the usual user of the laptop isn't available to provide the password.

Resolution for the recovery password for a laptop wasn't backed up

You can use either of the following methods to manually back up or synchronize an online client's existing recovery information:

- Create a Windows Management Instrumentation (WMI) script that backs up the information. For more information, see BitLocker Drive Encryption Provider.
- In an elevated Command Prompt window, use the manage-bde.exe command to back up the information.

  For example, to back up all of the recovery information for the C: drive to AD DS, open an elevated Command Prompt window and run the following command:

  ***cmd manage-bde.exe -protectors -adbackup C:

> **Note**
>
> BitLocker does not automatically manage this backup process.

Tablet devices don't support using `manage-bde.exe -forcerecovery` to test recovery mode

Consider the following scenario:

BitLocker recovery needs to be tested on a tablet or slate device by running the following command:

***cmd manage-bde.exe -forcerecovery

However, after entering the recovery password, the device can't start.

Cause of tablet devices don't support using `manage-bde.exe -forcerecovery` to test recovery mode

> **Important**

> Tablet devices do not support the `manage-bde.exe -forcerecovery` command.

This issue occurs because the Windows Boot Manager can't process touch-input during the pre-boot phase of startup. If Boot Manager detects that the device is a tablet, it redirects the startup process to the Windows Recovery Environment (WinRE), which can process touch-input.

If WindowsRE detects the TPM protector on the hard disk, it does a PCR reseal. However, the **`manage-bde.exe -forcerecovery`** command deletes the TPM protectors on the hard disk. Therefore, WinRE can't reseal the PCRs. This failure triggers an infinite BitLocker recovery cycle and prevents Windows from starting.

This behavior is by design for all versions of Windows.

Workaround for tablet devices don't support using `manage-bde.exe -forcerecovery` to test recovery mode

To resolve the restart loop, follow these steps:

1. On the BitLocker Recovery screen, select **Skip this drive**.
2. Select **Troubleshoot** > **Advanced Options** > **Command Prompt**.
3. In the Command Prompt window, run the following commands:

   cmd

   ```
   manage-bde.exe -unlock C: -rp <48-digit BitLocker recovery password>
   manage-bde.exe -protectors -disable C:
   ```

4. Close the Command Prompt window.
5. Shut down the device.
6. Start the device. Windows should start as usual.

After installing UEFI or TPM firmware updates on Surface, BitLocker prompts for the recovery password

Consider the following scenario:

A Surface device has BitLocker drive encryption turned on. The firmware of the Surface's TPM is updated or an update that changes the signature of the system firmware is installed. For example, the Surface TPM (IFX) update is installed.

You experience one or more of the following symptoms on the Surface device:

- At startup, the Surface device prompts for a BitLocker recovery password. The correct recovery password is entered, but Windows doesn't start up.
- Startup progresses directly into the Surface device's Unified Extensible Firmware Interface (UEFI) settings.
- The Surface device appears to be in an infinite restart loop.

Cause of after installing UEFI or TPM firmware updates on Surface, BitLocker prompts for the recovery password

This issue occurs if the Surface device TPM is configured to use Platform Configuration Register (PCR) values other than the default values of PCR 7 and PCR 11. For example, the following settings can configure the TPM this way:

- Secure boot is turned off.
- PCR values have been explicitly defined, such as by group policy.

Devices that support Connected Standby (also known as *InstantGO* or *Always On, Always Connected PCs*), including Surface devices, must use PCR 7 of the TPM. In its default configuration on such systems, BitLocker binds to PCR 7 and PCR 11 if PCR 7 and Secure Boot are correctly configured. For more information, see the BitLocker Group Policy Settings: About the Platform Configuration Register (PCR).

Resolution for after installing UEFI or TPM firmware updates on Surface, BitLocker prompts for the recovery password

To verify the PCR values that are in use on a device, open an elevated Command Prompt window and run the following command:

```
cmd
```

```
manage-bde.exe -protectors -get <OSDriveLetter>:
```

In this command, <*OSDriveLetter*> represents the drive letter of the operating system drive.

To resolve this issue and repair the device, follow these steps:

Step 1: Disable the TPM protectors on the boot drive

If a TPM or UEFI update has been installed and the Surface device can't start, even if the correct BitLocker recovery password has been entered, the ability to start can be restored by using the BitLocker recovery password and a Surface recovery image to remove the TPM protectors from the boot drive.

To use the BitLocker recovery password and a Surface recovery image to remove the TPM protectors from the boot drive, follow these steps:

1. Obtain the BitLocker recovery password from the Surface user's Microsoft.com account. If BitLocker is managed by a different method, such as Microsoft BitLocker Administration and Monitoring (MBAM), Configuration Manager BitLocker Management, or Intune, contact the administrator for help.
2. Use another computer to download the Surface recovery image from Surface Recovery Image Download. Use the downloaded image to create a USB recovery drive.
3. Insert the USB Surface recovery image drive into the Surface device, and start the device.
4. When prompted, select the following items:

   a. The operating system language.

   b. The keyboard layout.
5. Select **Troubleshoot** > **Advanced Options** > **Command Prompt**.
6. In the Command Prompt window, run the following commands:

   ```cmd
   manage-bde.exe -unlock -recoverypassword <Password> <DriveLetter>:
   manage-bde.exe -protectors -disable <DriveLetter>:
   ```

   where:

   - <*Password*> is the BitLocker recovery password that was obtained in Step 1

- <*DriveLetter*> is the drive letter that is assigned to the operating system drive

> ⓘ **Note**
>
> For more information about how to use this command, see **manage-bde unlock**.

7. Restart the computer.
8. When prompted, enter the BitLocker recovery password that was obtained in Step 1.

> ⓘ **Note**
>
> After the TPM protectors are disabled, BitLocker drive encryption no longer protects the device. To re-enable BitLocker drive encryption, select **Start**, type **Manage BitLocker**, and then press **Enter**. Follow the steps to encrypt the drive.

Step 2: Use Surface BMR to recover data and reset the Surface device

To recover data from the Surface device if Windows doesn't start, follow steps 1 through 5 of the section Step 1: Disable the TPM protectors on the boot drive to get to a Command Prompt window. Once a Command Prompt window is open, follow these steps:

1. At the command prompt, run the following command:

   ```cmd
   manage-bde.exe -unlock -recoverypassword <Password> <DriveLetter>:
   ```

   In this command, <*Password*> is the BitLocker recovery password that was obtained in Step 1 of the section Step 1: Disable the TPM protectors on the boot drive, and <*DriveLetter*> is the drive letter that is assigned to the operating system drive.

2. After the drive is unlocked, use the `copy` or `xcopy.exe` command to copy the user data to another drive.

   > ⓘ **Note**

> For more information about the these commands, see the **Windows commands** article.

3. To reset the device by using a Surface recovery image, follow the instructions in the article Creating and using a USB recovery drive for Surface.

Step 3: Restore the default PCR values

To prevent this issue from recurring, it's recommended to restore the default configuration of Secure Boot and the PCR values.

To enable Secure Boot on a Surface device, follow these steps:

1. Suspend BitLocker by opening an elevated Windows PowerShell window and running the following PowerShell cmdlet:

   ```PowerShell
   Suspend-BitLocker -MountPoint "<DriveLetter>:" -RebootCount 0
   ```

   In this command, *<DriveLetter>* is the letter that is assigned to the drive.

2. Restart the device, and then edit the UEFI settings to set the **Secure Boot** option to **Microsoft Only**.

3. Restart the device and sign into Windows.

4. Open an elevated PowerShell window and run the following PowerShell cmdlet:

   ```PowerShell
   Resume-BitLocker -MountPoint "<DriveLetter>:"
   ```

To reset the PCR settings on the TPM, follow these steps:

1. Disable any Group Policy Objects that configure the PCR settings, or remove the device from any groups that enforce such policies.

   For more information, see BitLocker Group Policy settings.

2. Suspend BitLocker by opening an elevated Windows PowerShell window and running the following PowerShell cmdlet:

   ```PowerShell
   ```

```
Suspend-BitLocker -MountPoint "<DriveLetter>:" -RebootCount 0
```

In this command, *<DriveLetter>* is the letter that is assigned to the drive.

3. Run the following PowerShell cmdlet:

```PowerShell
Resume-BitLocker -MountPoint "<DriveLetter>:"
```

Step 4: Suspend BitLocker during TPM or UEFI firmware updates

You can avoid this scenario when installing updates to system firmware or TPM firmware by temporarily suspending BitLocker before applying such updates.

> **ⓘ Important**
>
> TPM and UEFI firmware updates may require multiple restarts while they install. To keep BitLocker suspended during this process, the PowerShell cmdlet **Suspend-BitLocker** must be used and the **Reboot Count** parameter must be set to either of the following values:
>
> - **2** or greater: This value sets the number of times the device will restart before BitLocker Device Encryption resumes. For example, setting the value to **2** will cause BitLocker to resume after the device restarts twice.
> - **0**: This value suspends BitLocker Drive Encryption indefinitely. To resume BitLocker, the PowerShell cmdlet **Resume-BitLocker** or another mechanism needs to be used to resume BitLocker protection.

To suspend BitLocker while installing TPM or UEFI firmware updates:

1. Open an elevated Windows PowerShell window and run the following PowerShell cmdlet:

```PowerShell
Suspend-BitLocker -MountPoint "<DriveLetter>:" -RebootCount 0
```

In this PowerShell cmdlet, *<DriveLetter>* is the letter that is assigned to the drive.

2. Install the Surface device driver and firmware updates.

3. After installing the firmware updates, restart the computer, open an elevated PowerShell window, and then run the following PowerShell cmdlet:

```PowerShell
Resume-BitLocker -MountPoint "<DriveLetter>:"
```

Credential Guard/Device Guard on TPM 1.2: At every restart, BitLocker prompts for the recovery password and returns error 0xC0210000

Consider the following scenario:

A device uses TPM 1.2 and runs Windows 10, version 1809. The device also uses Virtualization-based Security features such as Device Guard and Credential Guard. Every time the device is started, the device enters BitLocker Recovery mode and an error message similar to the following error message is displayed:

> Recovery
>
> Your PC/Device needs to be repaired. A required file couldn't be accessed because your BitLocker key wasn't loaded correctly.
>
> Error code 0xc0210000
>
> You'll need to use recovery tools. If you don't have any installation media (like a disc or USB device), contact your PC administrator or PC/Device manufacturer.

Cause of Credential Guard/Device Guard on TPM 1.2: At every restart, BitLocker prompts for the recovery password and returns error 0xC0210000

TPM 1.2 doesn't support Secure Launch. For more information, see System Guard Secure Launch and SMM protection: Requirements Met by System Guard Enabled Machines

For more information about this technology, see Windows Defender System Guard: How a hardware-based root of trust helps protect Windows

Resolution for Credential Guard/Device Guard on TPM 1.2: At every restart, BitLocker prompts for the recovery password and returns error 0xC0210000

To resolve this issue, use one of the following two solutions:

- Remove any device that uses TPM 1.2 from any group that is subject to GPOs that enforce secure launch.
- Edit the **Turn On Virtualization Based Security** GPO to set **Secure Launch Configuration** to **Disabled**.

BitLocker Network Unlock: known issues

Article • 11/23/2022 • 4 minutes to read

By using the BitLocker Network Unlock feature, computers can be managed remotely without having to enter a BitLocker PIN when each computer starts up. To configure this behavior, the environment needs to meet the following requirements:

- Each computer belongs to a domain.
- Each computer has a wired connection to the internal network.
- The internal network uses DHCP to manage IP addresses.
- Each computer has a DHCP driver implemented in its Unified Extensible Firmware Interface (UEFI) firmware.

For general guidelines about how to troubleshoot BitLocker Network Unlock, see How to enable Network Unlock: Troubleshoot Network Unlock.

This article describes several known issues that may be encountered when BitLocker Network Unlock is used and provides guidance to address these issues.

Tip

BitLocker Network Unlock can be detected if it is enabled on a specific computer use the following steps on UEFI computers:

1. Open an elevated command prompt window and run the following command:

   ```
   cmd
   ```

   ```
   manage-bde.exe -protectors -get <Drive>
   ```

   For example:

   ```
   cmd
   ```

   ```
   manage-bde.exe -protectors -get C:
   ```

   If the output of this command includes a key protector of type **TpmCertificate (9)**, the configuration is correct for BitLocker Network Unlock.

2. Start Registry Editor, and verify the following settings:

   a. The following registry key exists and has the following value:

- **Subkey**: `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE`
- **Type**: `REG_DWORD`
- **Value**: `OSManageNKP` equal to `1` (True)

b. The registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\FVE_NKP\Certificates`

has an entry whose name matches the name of the certificate thumbprint of the BitLocker Network Unlock key protector that was found in step 1.

On a Surface Pro 4 device, BitLocker Network Unlock doesn't work because the UEFI network stack is incorrectly configured

Consider the following scenario:

BitLocker Network Unlock has been configured as described in BitLocker: How to enable Network Unlock. UEFI of a Surface Pro 4 has been configured to use DHCP. However, when the Surface Pro 4 is restarted, it still prompts for a BitLocker PIN.

When testing another device, such as a different type of tablet or laptop PC that's configured to use the same infrastructure, the device restarts as expected, without prompting for the BitLocker PIN. This test confirms that the infrastructure is correctly configured, and the issue is specific to the device.

Cause of BitLocker Network Unlock not working on Surface Pro 4

The UEFI network stack on the device is incorrectly configured.

Resolution for BitLocker Network Unlock not working on Surface Pro 4

To correctly configure the UEFI network stack of the Surface Pro 4, the Microsoft Surface Enterprise Management Mode (SEMM) needs to be used. For information about SEMM, see Enroll and configure Surface devices with SEMM.

> **Note**
>
> If SEMM can't be used, the Surface Pro 4 may be able to use BitLocker Network Unlock by configuring the Surface Pro 4 to use the network as its first boot option.

Unable to use BitLocker Network Unlock feature on a Windows client computer

Consider the following scenario:

BitLocker Network Unlock has been configured as described in BitLocker: How to enable Network Unlock. A Windows 8 client computer is connected to the internal network with an ethernet cable. However, when the device is restarted, the device still prompts for the BitLocker PIN.

Cause of unable to use BitLocker Network Unlock feature on a Windows client computer

A Windows 8-based or Windows Server 2012-based client computer sometimes doesn't receive or use the BitLocker Network Unlock protector, depending on whether the client receives unrelated BOOTP replies from a DHCP server or WDS server.

DHCP servers may send any DHCP options to a BOOTP client as allowed by the DHCP options and BOOTP vendor extensions. This behavior means that because a DHCP server supports BOOTP clients, the DHCP server replies to BOOTP requests.

The manner in which a DHCP server handles an incoming message depends in part on whether the message uses the Message Type option:

- The first two messages that the BitLocker Network Unlock client sends are DHCP DISCOVER\REQUEST messages. They use the Message Type option, so the DHCP server treats them as DHCP messages.
- The third message that the BitLocker Network Unlock client sends doesn't have the Message Type option. The DHCP server treats the message as a BOOTP request.

A DHCP server that supports BOOTP clients must interact with those clients according to the BOOTP protocol. The server must create a BOOTP BOOTREPLY message instead of a DHCP DHCPOFFER message. In other words, the server must not include the DHCP message option type and must not exceed the size limit for BOOTREPLY messages. After the server sends the BOOTP BOOTREPLY message, the server marks a binding for a

BOOTP client as BOUND. A non-DHCP client doesn't send a DHCPREQUEST message, nor does that client expect a DHCPACK message.

If a DHCP server that isn't configured to support BOOTP clients receives a BOOTREQUEST message from a BOOTP client, that server silently discards the BOOTREQUEST message.

For more information about DHCP and BitLocker Network Unlock, see BitLocker: How to enable Network Unlock: Network Unlock sequence.

Resolution for unable to use BitLocker Network Unlock feature on a Windows client computer

To resolve this issue, change the configuration of the DHCP server by changing the **DHCP** option from **DHCP and BOOTP** to **DHCP**.

Enforcing BitLocker policies by using Intune: known issues

Article • 11/23/2022 • 12 minutes to read

This article helps troubleshooting issues that may be experienced if using Microsoft Intune policy to manage silent BitLocker encryption on devices. The Intune portal indicates whether BitLocker has failed to encrypt one or more managed devices.



BitLockerFixedDrivesRecoveryOptions	Succeeded	
Warning for other disk encryption	Succeeded	
Encrypt devices	Error	-2016281112 (Remediation failed)
Allow standard users to enable encryption during Azure A...	Succeeded	
BitLockerFixedDrivesRequireEncryption	Succeeded	

To start narrowing down the cause of the problem, review the event logs as described in Troubleshoot BitLocker. Concentrate on the **Management** and **Operations** logs in the **Applications and Services logs** > **Microsoft** > **Windows** > **BitLocker-API** folder. The following sections provide more information about how to resolve the indicated events and error messages:

- Event ID 853: Error: A compatible Trusted Platform Module (TPM) Security Device cannot be found on this computer
- Event ID 853: Error: BitLocker Drive Encryption detected bootable media (CD or DVD) in the computer
- Event ID 854: WinRE is not configured
- Event ID 851: Contact manufacturer for BIOS upgrade
- Error message: The UEFI variable 'SecureBoot' could not be read
- Event ID 846, 778, and 851: Error 0x80072f9a
- Error message: There are conflicting group policy settings for recovery options on operating system drives

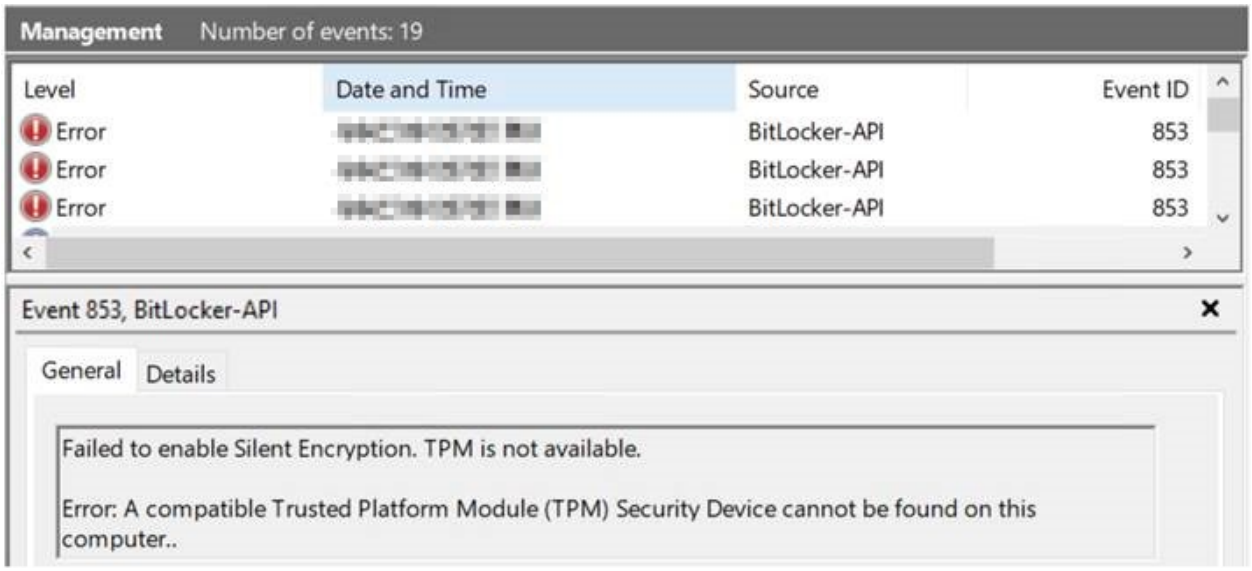
If there's no clear trail of events or error messages to follow, other areas to investigate include the following areas:

- Review the hardware requirements for using Intune to manage BitLocker on devices
- Review BitLocker policy configuration

For information about the procedure to verify whether Intune policies are enforcing BitLocker correctly, see Verifying that BitLocker is operating correctly.

Event ID 853: Error: A compatible Trusted Platform Module (TPM) Security Device cannot be found on this computer

Event ID 853 can carry different error messages, depending on the context. In this case, the Event ID 853 error message indicates that the device doesn't appear to have a TPM. The event information will be similar to the following event:



Cause of Event ID 853: Error: A compatible Trusted Platform Module (TPM) Security Device cannot be found on this computer

The device that is being secured may not have a TPM chip, or the device BIOS might have been configured to disable the TPM.

Resolution for Event ID 853: Error: A compatible Trusted Platform Module (TPM) Security Device cannot be found on this computer

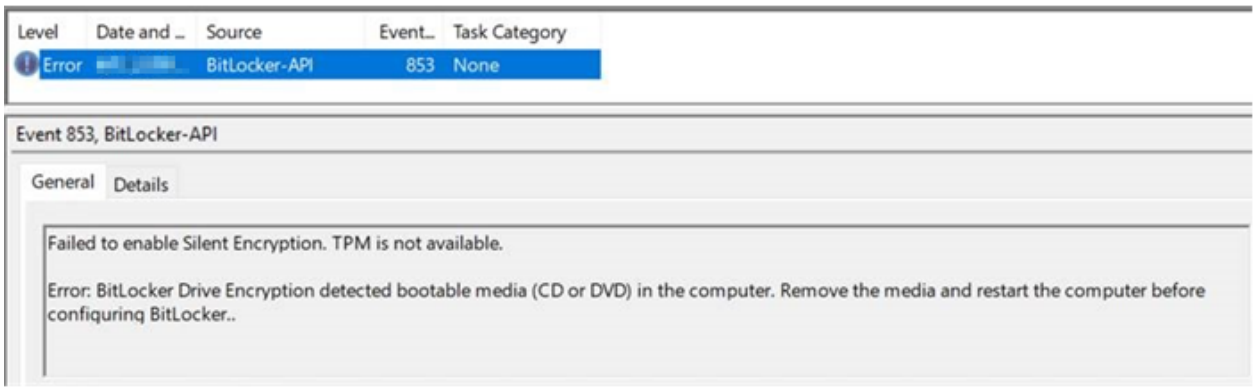
To resolve this issue, verify the following configurations:

- The TPM is enabled in the device BIOS.
- The TPM status in the TPM management console is similar to the following statuses:
  - Ready (TPM 2.0)
  - Initialized (TPM 1.2)

For more information, see Troubleshoot the TPM.

Event ID 853: Error: BitLocker Drive Encryption detected bootable media (CD or DVD) in the computer

In this case, event ID 853 is displayed, and the error message in the event indicates that bootable media is available to the device. The event information resembles the following.



Cause of Event ID 853: Error: BitLocker Drive Encryption detected bootable media (CD or DVD) in the computer

During the provisioning process, BitLocker drive encryption records the configuration of the device to establish a baseline. If the device configuration changes later (for example, if the media is removed), BitLocker recovery mode automatically starts.

To avoid this situation, the provisioning process stops if it detects a removable bootable media.

Resolution for Event ID 853: Error: BitLocker Drive Encryption detected bootable media (CD or DVD) in the computer

Remove the bootable media, and restart the device. After the device restarts, verify the encryption status.

Event ID 854: WinRE is not configured

The event information resembles the following error message:

> Failed to enable Silent Encryption. WinRe is not configured.
>
> Error: This PC cannot support device encryption because WinRE is not properly configured.

Cause of Event ID 854: WinRE is not configured

Windows Recovery Environment (WinRE) is a minimal Windows operating system that is based on Windows Preinstallation Environment (Windows PE). WinRE includes several tools that an administrator can use to recover or reset Windows and diagnose Windows issues. If a device can't start the regular Windows operating system, the device tries to start WinRE.

The provisioning process enables BitLocker drive encryption on the operating system drive during the Windows PE phase of provisioning. This action makes sure that the drive is protected before the full operating system is installed. The provisioning process also creates a system partition for WinRE to use if the system crashes.

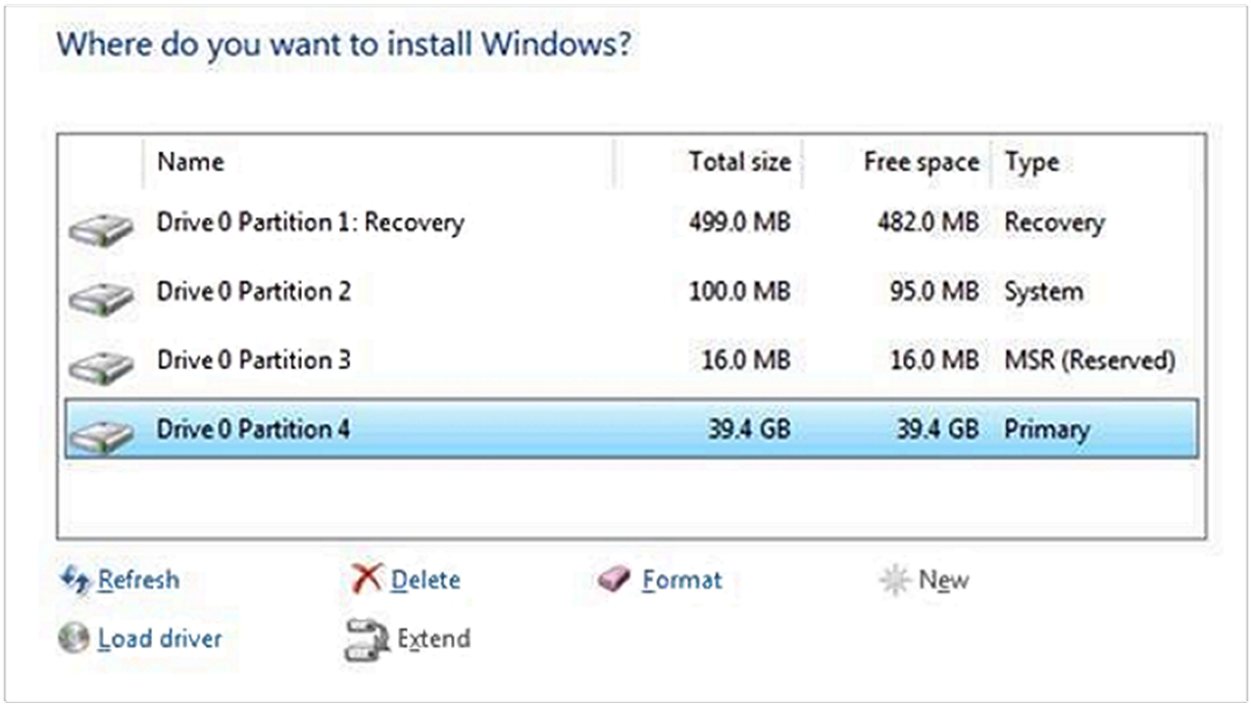
If WinRE isn't available on the device, provisioning stops.

Resolution for Event ID 854: WinRE is not configured

This issue can be resolved by verifying the configuration of the disk partitions, the status of WinRE, and the Windows Boot Loader configuration by following these steps:

Step 1: Verify the configuration of the disk partitions

The procedures described in this section depend on the default disk partitions that Windows configures during installation. Windows 11 and Windows 10 automatically create a recovery partition that contains the *Winre.wim* file. The partition configuration resembles the following.



To verify the configuration of the disk partitions, open an elevated Command Prompt window and run the following commands:

```cmd
diskpart.exe
list volume
```

```
C:\WINDOWS\system32>diskpart

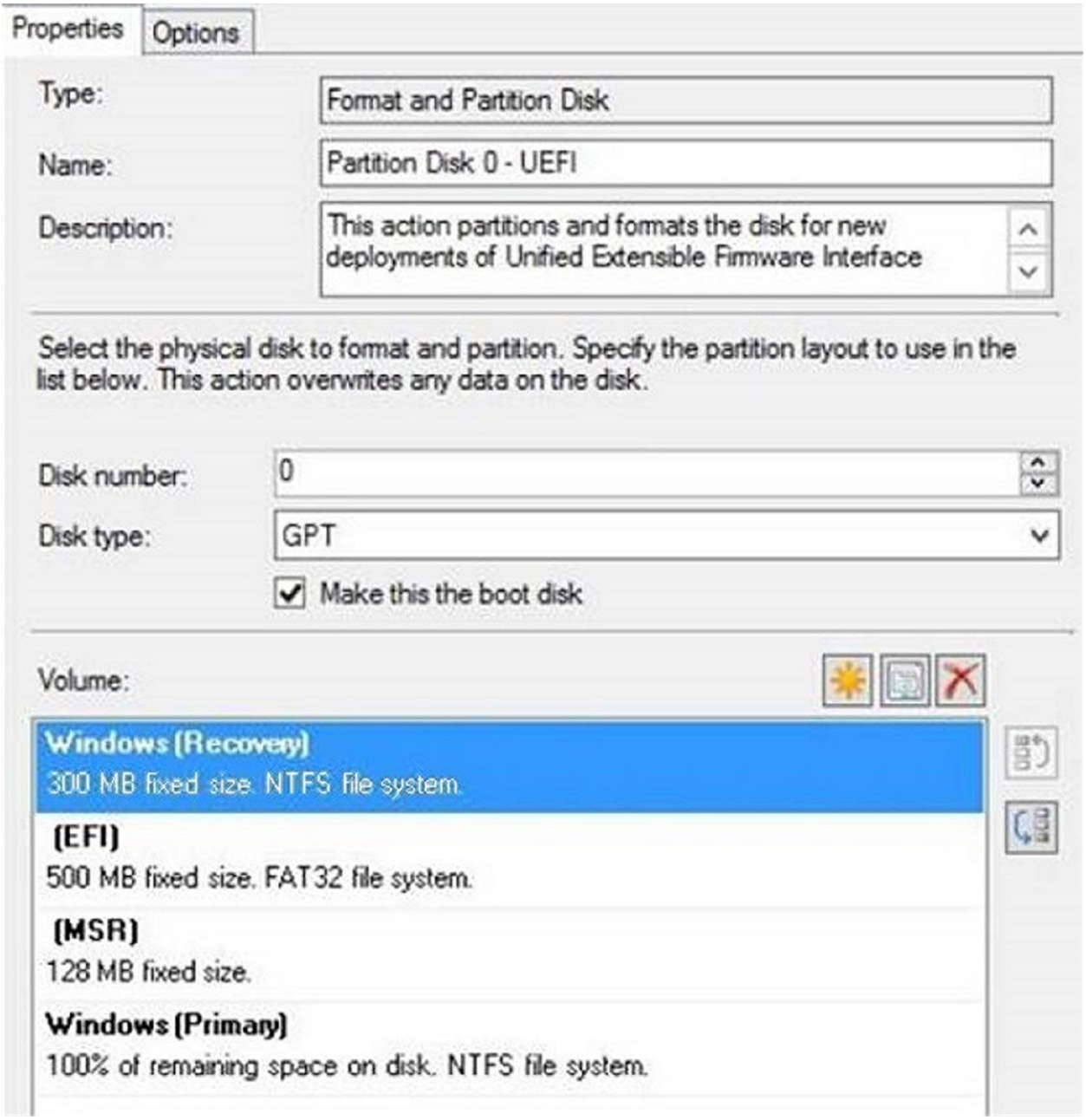
Microsoft DiskPart version 10.0.17763.1

Copyright (C) Microsoft Corporation.
On computer: MININT-8L1MASA

DISKPART> list vol

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     E                       DVD-ROM         0 B  No Media
  Volume 1         System       NTFS   Partition    499 MB  Healthy    System
  Volume 2     C   OSDisk       NTFS   Partition    216 GB  Healthy    Boot
  Volume 3     D   New Volume   NTFS   Partition    248 GB  Healthy
```

If the status of any of the volumes isn't healthy or if the recovery partition is missing, Windows may need to be reinstalled. Before reinstalling Windows, check the configuration of the Windows image that is being provisioned. Make sure that the image uses the correct disk configuration. The image configuration should resemble the following (this example is from Microsoft Configuration Manager):

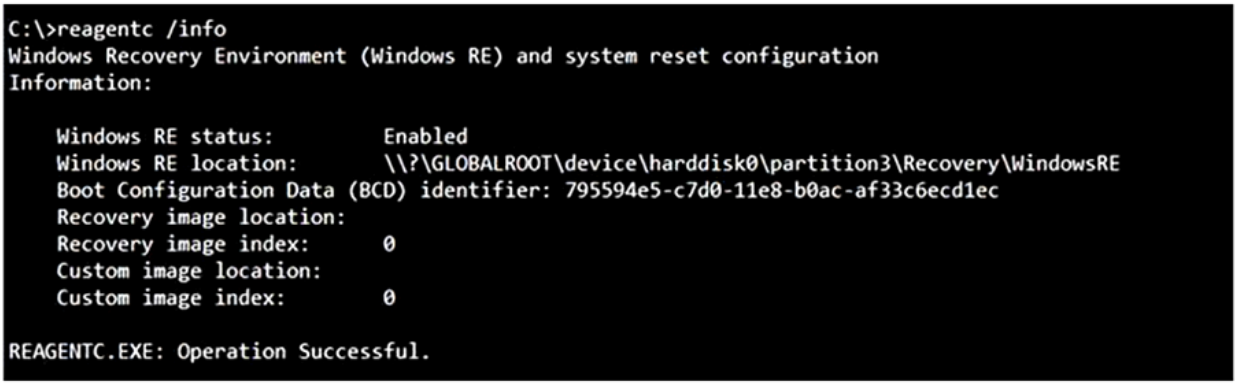


Step 2: Verify the status of WinRE

To verify the status of WinRE on the device, open an elevated Command Prompt window and run the following command:

```cmd
reagentc.exe /info
```

The output of this command resembles the following.



If the **Windows RE status** isn't **Enabled**, run the following command to enable it:

```
cmd

reagentc.exe /enable
```

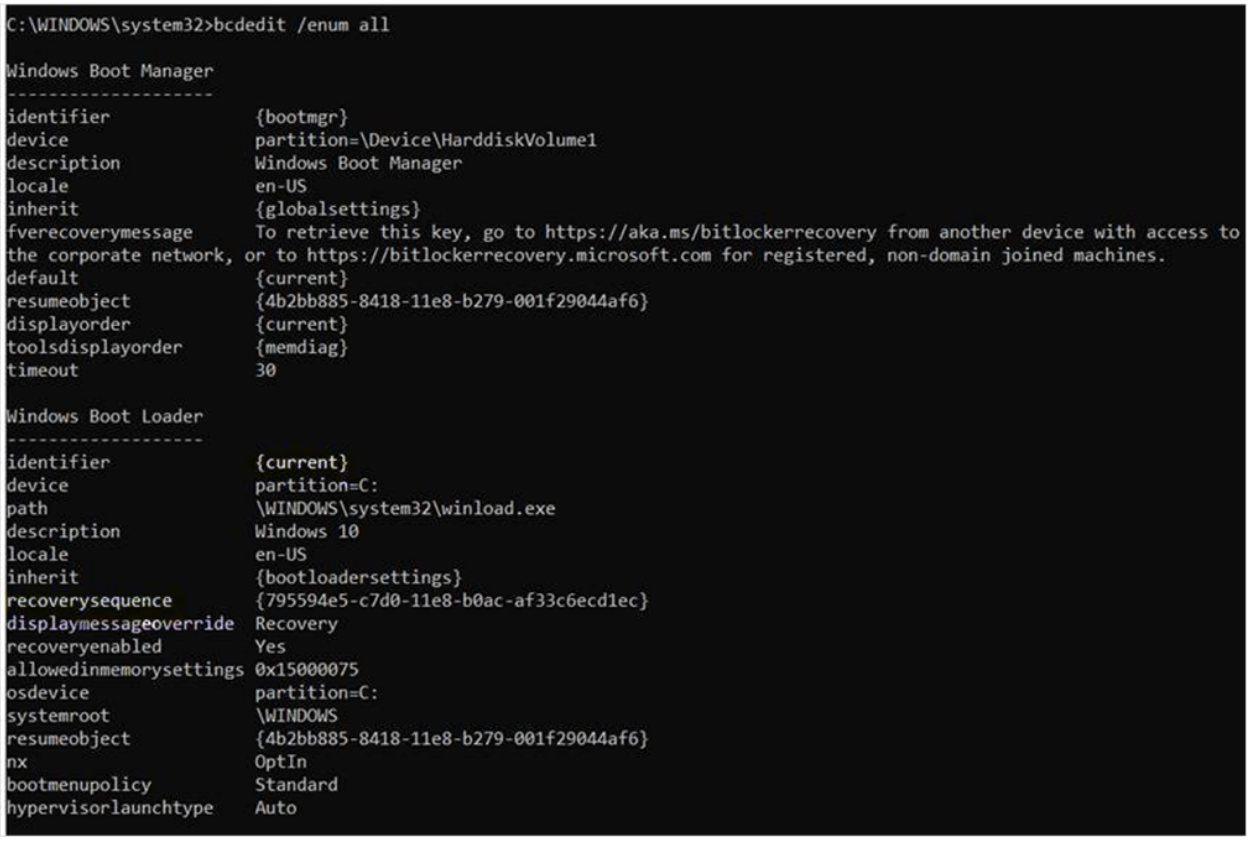
Step 3: Verify the Windows Boot Loader configuration

If the partition status is healthy, but the *reagentc.exe /enable* command results in an error, verify whether the Windows Boot Loader contains the recovery sequence GUID by running the following command in an elevated Command Prompt window:

```
cmd

bcdedit.exe /enum all
```

The output of this command will be similar to the following output:



```
C:\WINDOWS\system32>bcdedit /enum all

Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=\Device\HarddiskVolume1
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
fverecoverymessage      To retrieve this key, go to https://aka.ms/bitlockerrecovery from another device with access to
the corporate network, or to https://bitlockerrecovery.microsoft.com for registered, non-domain joined machines.
default                 {current}
resumeobject            {4b2bb885-8418-11e8-b279-001f29044af6}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \WINDOWS\system32\winload.exe
description             Windows 10
locale                  en-US
inherit                 {bootloadersettings}
recoverysequence        {795594e5-c7d0-11e8-b0ac-af33c6ecd1ec}
displaymessageoverride  Recovery
recoveryenabled         Yes
allowedinmemorysettings 0x15000075
osdevice                partition=C:
systemroot              \WINDOWS
resumeobject            {4b2bb885-8418-11e8-b279-001f29044af6}
nx                      OptIn
bootmenupolicy          Standard
hypervisorlaunchtype    Auto
```

In the output, locate the **Windows Boot Loader** section that includes the line **identifier={current}**. In that section, locate the **recoverysequence** attribute. The value of this attribute should be a GUID value, not a string of zeros.

Event ID 851: Contact the manufacturer for BIOS upgrade instructions

The event information will be similar to the following error message:

> Failed to enable Silent Encryption.
>
> Error: BitLocker Drive Encryption cannot be enabled on the operating system drive. Contact the computer manufacturer for BIOS upgrade instructions.

Cause of Event ID 851: Contact the manufacturer for BIOS upgrade instructions

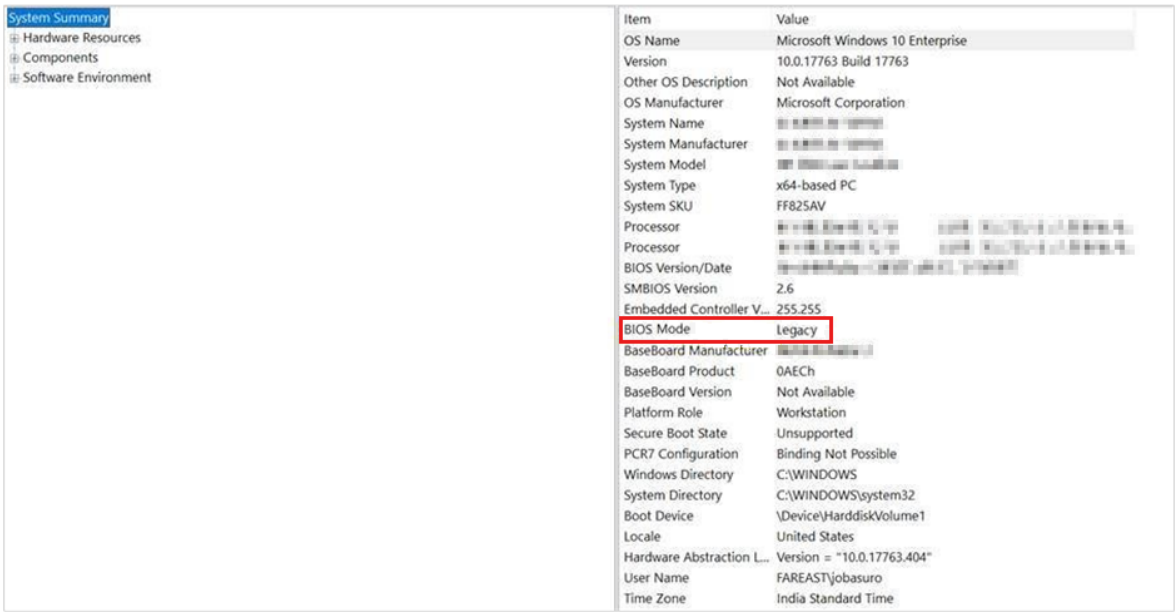
The device must have Unified Extensible Firmware Interface (UEFI) BIOS. Silent BitLocker drive encryption doesn't support legacy BIOS.

Resolution for Event ID 851: Contact the manufacturer for BIOS upgrade instructions

To verify the BIOS mode, use the System Information application by following these steps:

1. Select **Start**, and enter **msinfo32** in the **Search** box.

2. Verify that the **BIOS Mode** setting is **UEFI** and not **Legacy**.



3. If the **BIOS Mode** setting is **Legacy**, the UEFI firmware needs to be switched to **UEFI** or **EFI** mode. The steps for switching to **UEFI** or **EFI** mode are specific to the device.

> ⓘ **Note**
>
> If the device supports only Legacy mode, Intune can't be used to manage BitLocker Device Encryption on the device.

Error message: The UEFI variable 'SecureBoot' could not be read

An error message similar to the following error message is displayed:

> **Error:** BitLocker cannot use Secure Boot for integrity because the UEFI variable 'SecureBoot' could not be read. A required privilege is not held by the client.

Cause of Error message: The UEFI variable 'SecureBoot' could not be read

A platform configuration register (PCR) is a memory location in the TPM. In particular, PCR 7 measures the state of secure boot. Silent BitLocker drive encryption requires the secure boot to be turned on.

Resolution for Error message: The UEFI variable 'SecureBoot' could not be read

This issue can be resolved by verifying the PCR validation profile of the TPM and the secure boot state by following these steps:

Step 1: Verify the PCR validation profile of the TPM

To verify that PCR 7 is in use, open an elevated Command Prompt window and run the following command:

```
cmd

Manage-bde.exe -protectors -get %systemdrive%
```

In the TPM section of the output of this command, verify whether the **PCR Validation Profile** setting includes **7**, as follows:



If **PCR Validation Profile** doesn't include **7** (for example, the values include **0**, **2**, **4**, and **11**, but not **7**), then secure boot isn't turned on.

```
C:\WINDOWS\system32>manage-bde -protectors -get %systemdrive%
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Volume C: [OSDisk]
All Key Protectors

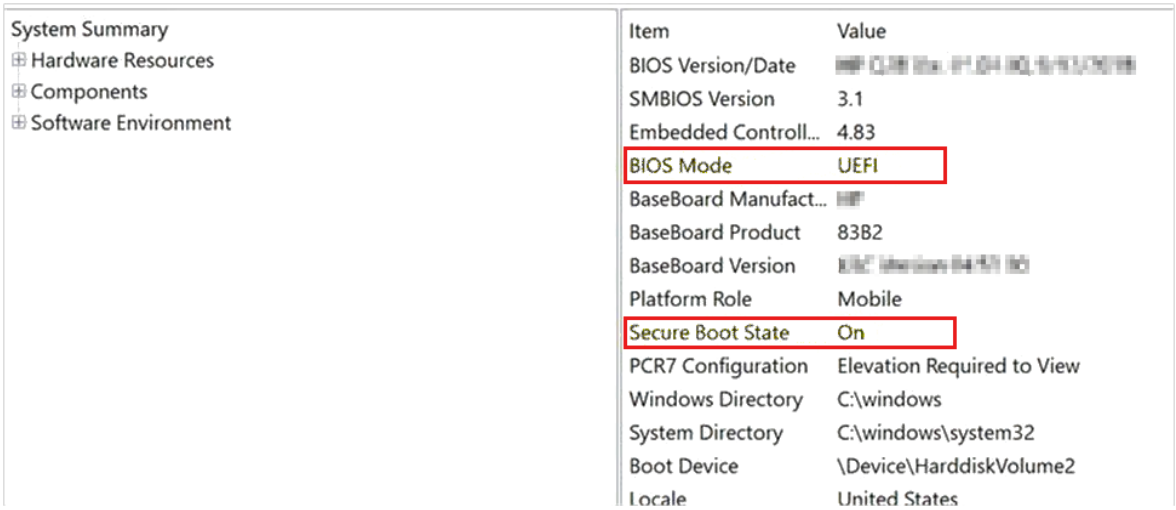
    Numerical Password:
      ID: {[redacted]}
      Password:


    TPM:
      ID: {[redacted]}
      PCR Validation Profile:
        0, 2, 4, 8, 9, 10, 11
```

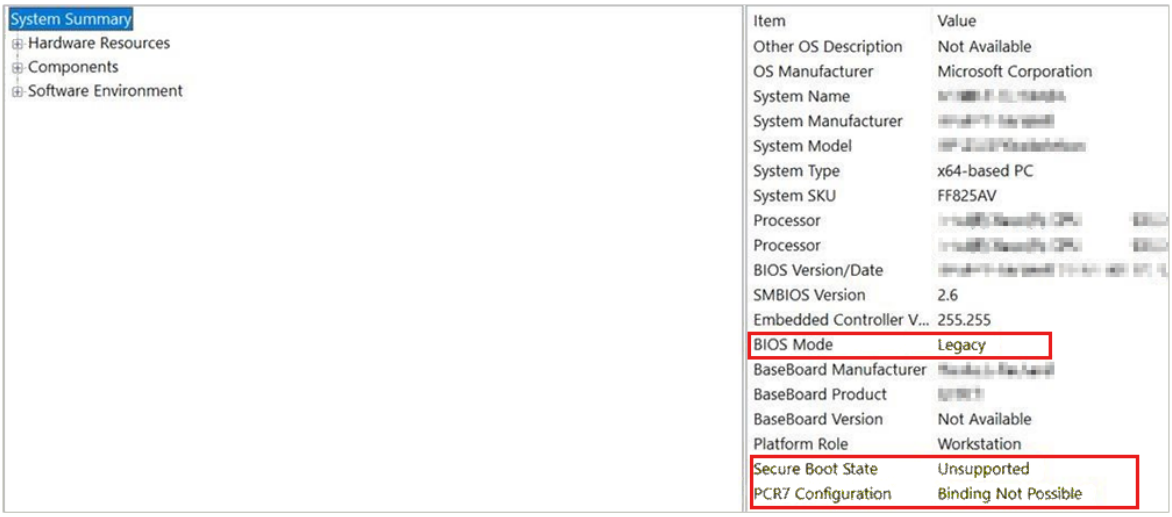
2: Verify the secure boot state

To verify the secure boot state, use the System Information application by following these steps:

1. Select **Start**, and enter **msinfo32** in the **Search** box.
2. Verify that the **Secure Boot State** setting is **On**, as follows:



3. If the **Secure Boot State** setting is **Unsupported**, Silent BitLocker Encryption can't be used on the device.



> **Note**
>
> The **Confirm-SecureBootUEFI** PowerShell cmdlet can also be used to verify the Secure Boot state by opening an elevated PowerShell window and running the following command:
>
> ```
> PowerShell
> ```
>
> ```
> Confirm-SecureBootUEFI
> ```
>
> If the computer supports Secure Boot and Secure Boot is enabled, this cmdlet returns "True."
>
> If the computer supports secure boot and secure boot is disabled, this cmdlet returns "False."
>
> If the computer does not support Secure Boot or is a BIOS (non-UEFI) computer, this cmdlet returns "Cmdlet not supported on this platform."

Event ID 846, 778, and 851: Error 0x80072f9a

Consider the following scenario:

Intune policy is being deployed to encrypt a Windows 10, version 1809 device, and the recovery password is being stored in Azure Active Directory (Azure AD). As part of the policy configuration, the **Allow standard users to enable encryption during Azure AD Join** option has been selected.

The policy deployment fails and the failure generates the following events in Event Viewer in the **Applications and Services Logs** > **Microsoft** > **Windows** > **BitLocker API**

folder:

> Event ID:846
>
> Event: Failed to backup BitLocker Drive Encryption recovery information for volume C: to your Azure AD.
>
> TraceId: {cbac2b6f-1434-4faa-a9c3-597b17c1dfa3} Error: Unknown HResult Error code: 0x80072f9a

> Event ID:778
>
> Event: The BitLocker volume C: was reverted to an unprotected state.

> Event ID: 851
>
> Event: Failed to enable Silent Encryption.
>
> Error: Unknown HResult Error code: 0x80072f9a.

These events refer to Error code 0x80072f9a.

Cause of Event ID 846, 778, and 851: Error 0x80072f9a

These events indicate that the signed-in user doesn't have permission to read the private key on the certificate that is generated as part of the provisioning and enrollment process. Therefore, the BitLocker MDM policy refresh fails.

The issue affects Windows 10 version 1809.

Resolution for Event ID 846, 778, and 851: Error 0x80072f9a

To resolve this issue, install the May 21, 2019 update.

Error message: There are conflicting group policy settings for recovery options on operating system drives

An error message similar to the following error message is displayed:

> **Error:** BitLocker Drive Encryption cannot be applied to this drive because there are conflicting Group Policy settings for recovery options on operating system drives. Storing recovery information to Active Directory Domain Services cannot be required when the generation of recovery passwords is not permitted. Please have your system administrator resolve these policy conflicts before attempting to enable BitLocker...

Resolution for Error message: There are conflicting group policy settings for recovery options on operating system drives

To resolve this issue, review the group policy object (GPO) settings for conflicts. For more information, see the next section, Review BitLocker policy configuration.

For more information about GPOs and BitLocker, see BitLocker Group Policy Reference.

Review BitLocker policy configuration

For information about the procedure to use policy together with BitLocker and Intune, see the following resources:

- BitLocker management for enterprises: Managing devices joined to Azure Active Directory
- BitLocker Group Policy Reference
- Configuration service provider reference
- Policy CSP – BitLocker
- BitLocker CSP
- Enable ADMX-backed policies in MDM
- gpresult

Intune offers the following enforcement types for BitLocker:

- **Automatic** (Enforced when the device joins Azure AD during the provisioning process. This option is available in Windows 10 version 1703 and later.)
- **Silent** (Endpoint protection policy. This option is available in Windows 10 version 1803 and later.)
- **Interactive** (Endpoint policy for Windows versions that are older than Windows 10 version 1803.)

If the device runs Windows 10 version 1703 or later, supports Modern Standby (also known as Instant Go) and is HSTI-compliant, joining the device to Azure AD triggers

automatic device encryption. A separate endpoint protection policy isn't required to enforce device encryption.

If the device is HSTI-compliant but doesn't support Modern Standby, an endpoint protection policy has to be configured to enforce silent BitLocker drive encryption. The settings for this policy should be similar to the following settings:



The OMA-URI references for these settings are as follows:

- OMA-URI: **./Device/Vendor/MSFT/BitLocker/RequireDeviceEncryption**
  Value Type: **Integer**
  Value: **1** (1 = Require, 0 = Not Configured)
- OMA-URI:
  ./Device/Vendor/MSFT/BitLocker/AllowWarningForOtherDiskEncryption
  Value Type: **Integer**
  Value: **0** (0 = Blocked, 1 = Allowed)

> ⓘ **Note**
>
> Because of an update to the BitLocker Policy CSP, if the device uses Windows 10 version 1809 or later, an endpoint protection policy can be used to enforce silent BitLocker Device Encryption even if the device is not HSTI-compliant.

> ⓘ **Note**
>
> If the **Warning for other disk encryption** setting is set to **Not configured**, the BitLocker drive encryption wizard has to be manually started.

If the device doesn't support Modern Standby but is HSTI-compliant, and it uses a version of Windows that is earlier than Windows 10, version 1803, an endpoint protection policy that has the settings that are described in this article delivers the policy configuration to the device. However, Windows then notifies the user to manually enable BitLocker Drive Encryption. When the user selects the notification, it will start the BitLocker Drive Encryption wizard.

Intune provides settings that can be used to configure automatic device encryption for Autopilot devices for standard users. Each device must meet the following requirements:

- Be HSTI-compliant
- Support Modern Standby
- Use Windows 10 version 1803 or later



The OMA-URI references for these settings are as follows:

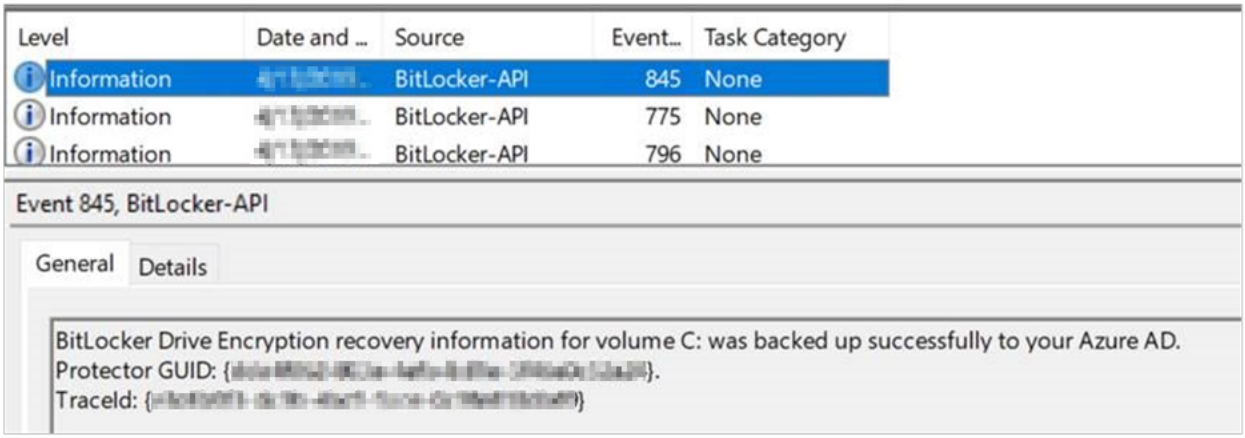
- OMA-URI: **./Device/Vendor/MSFT/BitLocker/AllowStandardUserEncryption**
  Value Type: **Integer** Value: **1**

> ⓘ **Note**
>
> This node works together with the **RequireDeviceEncryption** and **AllowWarningForOtherDiskEncryption** nodes. For this reason, when the following settings are set:
>
> - **RequireDeviceEncryption** to **1**
> - **AllowStandardUserEncryption** to **1**
> - **AllowWarningForOtherDiskEncryption** to **0**
>
> Intune enforces silent BitLocker encryption for Autopilot devices that have standard user profiles.

Verifying that BitLocker is operating correctly

During regular operations, BitLocker drive encryption generates events such as Event ID 796 and Event ID 845.



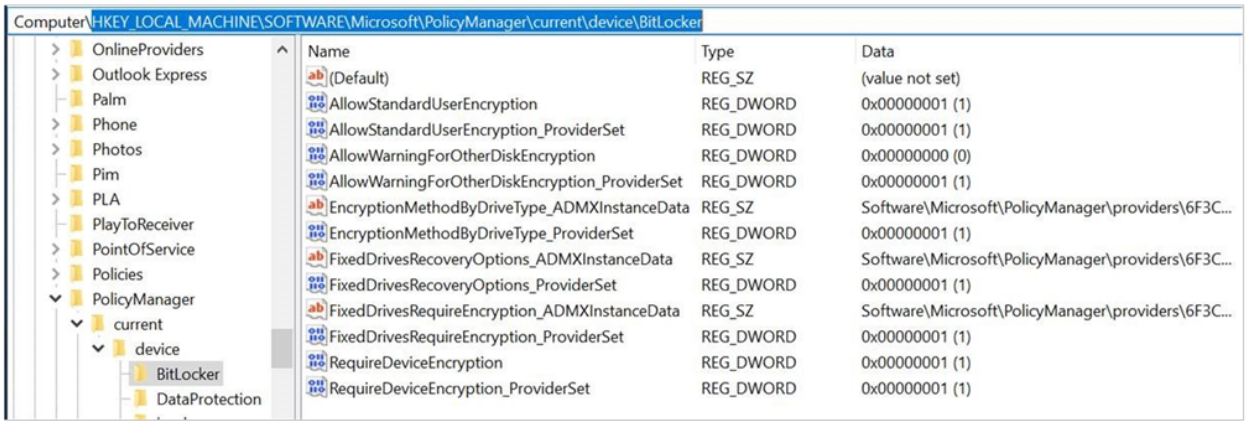


It can also be determined whether the BitLocker recovery password has been uploaded to Azure AD by checking the device details in the Azure AD Devices section.



On the device, check the Registry Editor to verify the policy settings on the device. Verify the entries under the following subkeys:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device\BitLocker`
- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device`


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device\BitLocker
OnlineProviders
Outlook Express
Palm
Phone
Photos
Pim
PLA
PlayToReceiver
PointOfService
Policies
PolicyManager
current
device
BitLocker
DataProtection
Name
Type
Data
(Default)
REG_SZ
(value not set)
AllowStandardUserEncryption
REG_DWORD
0x00000001 (1)
AllowStandardUserEncryption_ProviderSet
REG_DWORD
0x00000001 (1)
AllowWarningForOtherDiskEncryption
REG_DWORD
0x00000000 (0)
AllowWarningForOtherDiskEncryption_ProviderSet
REG_DWORD
0x00000001 (1)
EncryptionMethodByDriveType_ADMXInstanceData
REG_SZ
Software\Microsoft\PolicyManager\providers\6F3C...
EncryptionMethodByDriveType_ProviderSet
REG_DWORD
0x00000001 (1)
FixedDrivesRecoveryOptions_ADMXInstanceData
REG_SZ
Software\Microsoft\PolicyManager\providers\6F3C...
FixedDrivesRecoveryOptions_ProviderSet
REG_DWORD
0x00000001 (1)
FixedDrivesRequireEncryption_ADMXInstanceData
REG_SZ
Software\Microsoft\PolicyManager\providers\6F3C...
FixedDrivesRequireEncryption_ProviderSet
REG_DWORD
0x00000001 (1)
RequireDeviceEncryption
REG_DWORD
0x00000001 (1)
RequireDeviceEncryption_ProviderSet
REG_DWORD
0x00000001 (1)

BitLocker cannot encrypt a drive: known issues

Article • 11/23/2022 • 2 minutes to read

This article describes common issues that prevent BitLocker from encrypting a drive. This article also provides guidance to address these issues.

> **Note**
>
> If it is determined that the BitLocker issue involves the trusted platform module (TPM), see **BitLocker cannot encrypt a drive: known TPM issues**.

Error 0x80310059: BitLocker drive encryption is already performing an operation on this drive

When BitLocker Drive Encryption is turned on a computer that is running Windows 10 Professional or Windows 11, the following message may appear:

> ERROR: An error occurred (code 0x80310059): BitLocker Drive Encryption is already performing an operation on this drive. Please complete all operations before continuing. NOTE: If the -on switch has failed to add key protectors or start encryption, you may need to call manage-bde -off before attempting -on again.

Cause of Error 0x80310059

This issue may be caused by settings that are controlled by group policy objects (GPOs).

Resolution for Error 0x80310059

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if the registry is modified incorrectly. Before modifying the registry, **back up the registry for restoration** in case problems occur.

To resolve this issue, follow these steps:

1. Start Registry Editor, and navigate to the following subkey:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE`

2. Delete the following entries:

   - `OSPlatformValidation_BIOS`
   - `OSPlatformValidation_UEFI`
   - `PlatformValidation`

3. Exit registry editor, and turn on BitLocker drive encryption again.

Guidelines for troubleshooting BitLocker

Article • 11/23/2022 • 4 minutes to read

This article addresses common issues in BitLocker and provides guidelines to troubleshoot these issues. This article also provides information such as what data to collect and what settings to check. This information makes the troubleshooting process much easier.

Review the event logs

Open **Event Viewer** and review the following logs under **Applications and Services Logs** > **Microsoft** > **Windows**:

- **BitLocker-API**. Review the **Management** log, the **Operational** log, and any other logs that are generated in this folder. The default logs have the following unique names:
  - **Microsoft-Windows-BitLocker-API/Management**
  - **Microsoft-Windows-BitLocker-API/Operational**
  - **Microsoft-Windows-BitLocker-API/Tracing** - only displayed when **Show Analytic and Debug Logs** is enabled

- **BitLocker-DrivePreparationTool**. Review the **Admin** log, the **Operational** log, and any other logs that are generated in this folder. The default logs have the following unique names:
  - **Microsoft-Windows-BitLocker-DrivePreparationTool/Admin**
  - **Microsoft-Windows-BitLocker-DrivePreparationTool/Operational**

Additionally, review the **Windows Logs** > **System** log for events that were produced by the TPM and TPM-WMI event sources.

To filter and display or export logs, the wevtutil.exe command-line tool or the Get-WinEvent PowerShell cmdlet can be used.

For example, to use *wevtutil.exe* to export the contents of the operational log from the BitLocker-API folder to a text file that is named *BitLockerAPIOpsLog.txt*, open a Command Prompt window, and run the following command:

```
cmd
```

```
wevtutil.exe qe "Microsoft-Windows-BitLocker/BitLocker Operational" /f:text
> BitLockerAPIOpsLog.txt
```

To use the **Get-WinEvent** cmdlet to export the same log to a comma-separated text file, open a Windows PowerShell window and run the following command:

PowerShell

```
Get-WinEvent -logname "Microsoft-Windows-BitLocker/BitLocker Operational"  |
Export-Csv -Path Bitlocker-Operational.csv
```

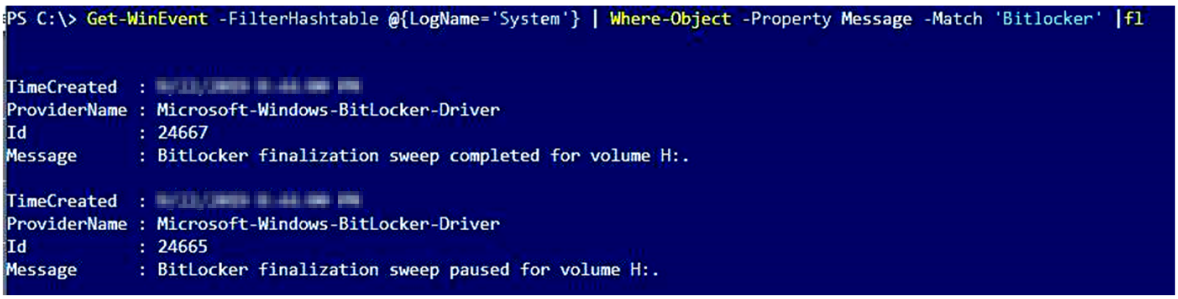
The Get-WinEvent can be used in an elevated PowerShell window to display filtered information from the system or application log by using the following syntax:

- To display BitLocker-related information:

  PowerShell

  ```
  Get-WinEvent -FilterHashtable @{LogName='System'} | Where-Object -
  Property Message -Match 'BitLocker' | fl
  ```

  The output of such a command resembles the following:

- To export BitLocker-related information:

  PowerShell

  ```
  Get-WinEvent -FilterHashtable @{LogName='System'} | Where-Object -
  Property Message -Match 'BitLocker' | Export-Csv -Path System-
  BitLocker.csv
  ```

- To display TPM-related information:

  PowerShell

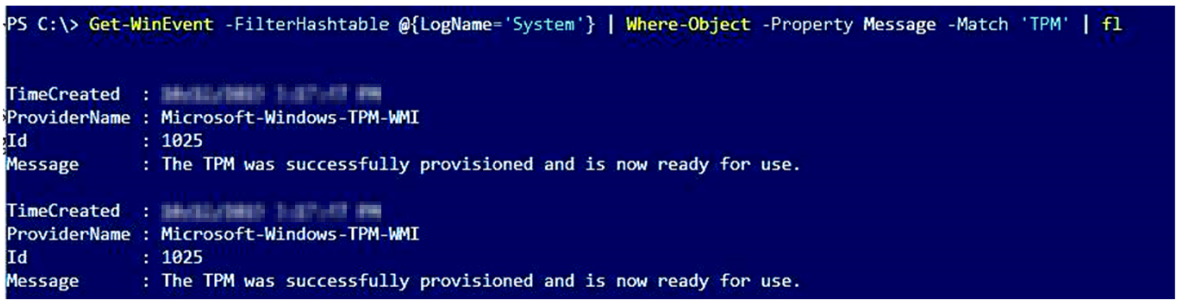
  ```
  Get-WinEvent -FilterHashtable @{LogName='System'} | Where-Object -
  Property Message -Match 'TPM' | fl
  ```

- To export TPM-related information:

  PowerShell

  ```
  Get-WinEvent -FilterHashtable @{LogName='System'} | Where-Object -
  Property Message -Match 'TPM' | Export-Csv -Path System-TPM.csv
  ```

  The output of such a command resembles the following.



> **Note**
>
> When contacting Microsoft Support, it is recommended to export the logs listed in this section.

Gather status information from the BitLocker technologies

Open an elevated Windows PowerShell window, and run each of the following commands:

Command	Notes	More Info
`Get-Tpm > C:\TPM.txt`	PowerShell cmdlet that exports information about the local computer's Trusted Platform Module (TPM). This cmdlet shows different values depending on whether the TPM chip is version 1.2 or 2.0. This cmdlet isn't supported in Windows 7.	Get-Tpm
`manage-bde.exe -status > C:\BDEStatus.txt`	Exports information about the general encryption status of all drives on the computer.	manage-bde.exe status
`manage-bde.exe c: -protectors -get > C:\Protectors`	Exports information about the protection methods that are used for the BitLocker encryption key.	manage-bde.exe protectors

Command	Notes	More Info
`reagentc.exe /info > C:\reagent.txt`	Exports information about an online or offline image about the current status of the Windows Recovery Environment (WindowsRE) and any available recovery image.	reagentc.exe
`Get-BitLockerVolume | fl`	PowerShell cmdlet that gets information about volumes that BitLocker Drive Encryption can protect.	Get-BitLockerVolume

Review the configuration information

1. Open an elevated Command Prompt window, and run the following commands:

Command	Notes	More Info
`gpresult.exe /h <Filename>`	Exports the Resultant Set of Policy information, and saves the information as an HTML file.	gpresult.exe
`msinfo.exe /report <Path> /computer <ComputerName>`	Exports comprehensive information about the hardware, system components, and software environment on the local computer. The **/report** option saves the information as a .txt file.	msinfo.exe

2. Open Registry Editor, and export the entries in the following subkeys:

   - `HKLM\SOFTWARE\Policies\Microsoft\FVE`
   - `HKLM\SYSTEM\CurrentControlSet\Services\TPM\`

Check the BitLocker prerequisites

Common settings that can cause issues for BitLocker include the following scenarios:

- The TPM must be unlocked. Check the output of the *get-tpm* PowerShell cmdlet command for the status of the TPM.
- Windows RE must be enabled. Check the output of the *reagentc.exe* command for the status of WindowsRE.
- The system-reserved partition must use the correct format.
  - On Unified Extensible Firmware Interface (UEFI) computers, the system-reserved partition must be formatted as FAT32.
  - On legacy computers, the system-reserved partition must be formatted as NTFS.

- If the device being troubleshot is a slate or tablet PC, use https://gpsearch.azurewebsites.net/#8153 to verify the status of the **Enable use of BitLocker authentication requiring preboot keyboard input on slates** option.

For more information about the BitLocker prerequisites, see BitLocker basic deployment: Using BitLocker to encrypt volumes

Next steps

If the information examined so far indicates a specific issue (for example, WindowsRE isn't enabled), the issue may have a straightforward fix.

Resolving issues that don't have obvious causes depends on exactly which components are involved and what behavior is being see. The gathered information helps narrow down the areas to investigate.

- If the device being troubleshot is managed by Microsoft Intune, see Enforcing BitLocker policies by using Intune: known issues.
- If BitLocker doesn't start or can't encrypt a drive and errors or events that are related to the TPM are occurring, see BitLocker cannot encrypt a drive: known TPM issues.
- If BitLocker doesn't start or can't encrypt a drive, see BitLocker cannot encrypt a drive: known issues.
- If BitLocker Network Unlock doesn't behave as expected, see BitLocker Network Unlock: known issues.
- If BitLocker doesn't behave as expected when an encrypted drive is recovered, or if BitLocker unexpectedly recovered a drive, see BitLocker recovery: known issues.
- If BitLocker or the encrypted drive doesn't behave as expected, and errors or events that are related to the TPM are occurring, see BitLocker and TPM: other known issues.
- If BitLocker or the encrypted drive doesn't behave as expected, see BitLocker configuration: known issues.

It's recommended to keep the gathered information handy in case Microsoft Support is contacted for help with resolving the issue.

BitLocker Recovery starts when OEMs perform firmware updates for TPM 1.2

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for the issue where BitLocker Recovery starts when OEMs perform firmware updates for TPM 1.2.

Applies to: Windows 10 - all editions
Original KB number: 3184518

Symptoms

For Trusted Platform Module (TPM) 1.2, Windows does not know if the system is going through a firmware update. In this situation, the computer reboots into BitLocker Recovery.

Manage-bde: protectors

To suspend protection, run the following command line:

```
Console

manage-bde -protectors -disable c:
```

To resume protection, run the following command line:

```
Console

manage-bde -protectors -enable c:
```

Workaround

For IT managers who are performing firmware updates for TPM 1.2 through Windows Update, make sure that you suspend BitLocker before you run the updates. This prevents BitLocker Recovery from starting.

More Information

Use TPM 2.0, as PCR 7 performs all these measurements automatically.

Earlier Windows versions don't start after "Setup Windows and Configuration Manager" step if Pre-Provision BitLocker is used with Windows 10, version 1511

Article • 03/24/2022 • 2 minutes to read

This article explains why earlier Windows versions don't start after you run the "Setup Windows and Configuration Manager" step if Pre-Provision BitLocker is used with Windows 10, version 1511.

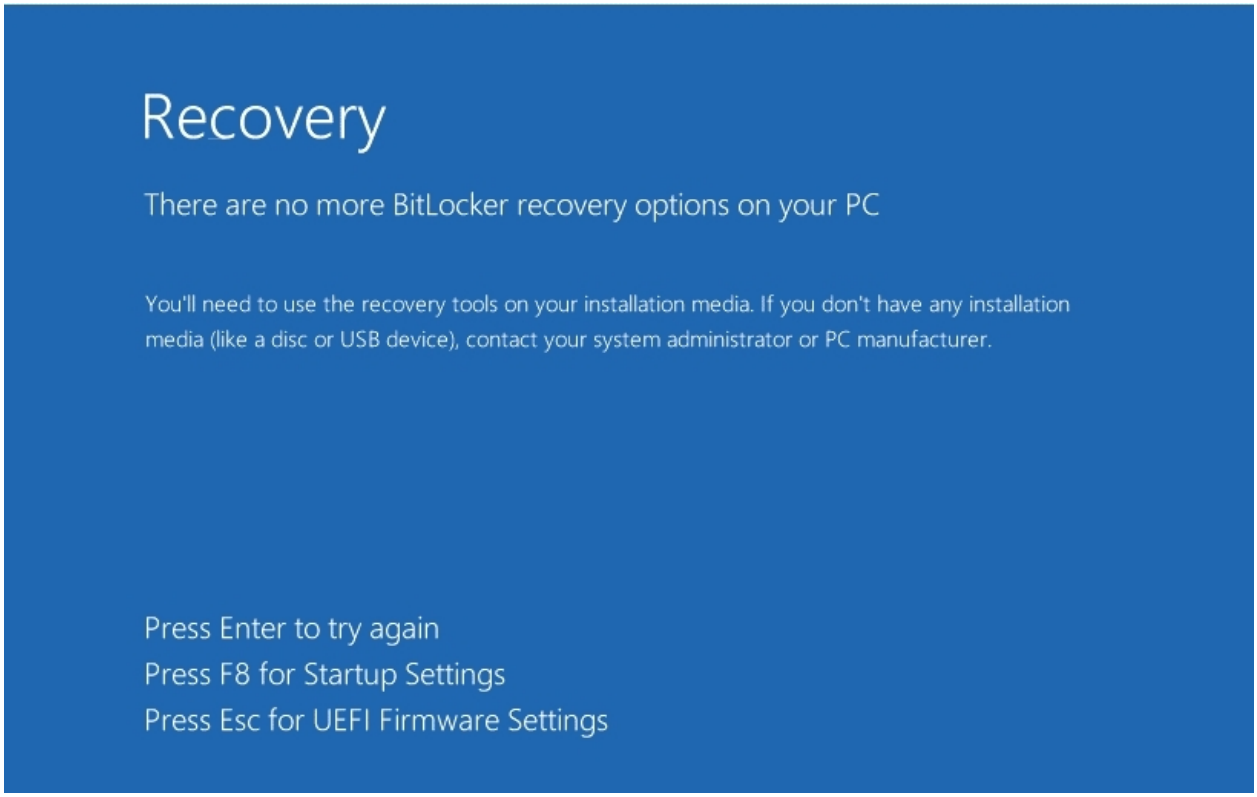
Applies to: Windows 10 – all editions, Windows 7 Service Pack 1
Original KB number: 4494799

Symptoms

Consider following scenario:

- You install the Windows 10, version 1511 ADK to your boot images.
- You apply KB3143760 to your boot images.
- You want to install a Windows version that's earlier than Windows 10, version 1511 by using your new 1511 boot images. To do this, you add the built-in "Pre-Provision BitLocker" step to your task sequence. This enables the "Used space only encryption" feature to speed up BitLocker drive encryption.

All the steps in the task sequence work as expected until the "Setup Windows and Configuration Manager" step. After this step runs, your device starts up into a "Recovery" screen that displays a "There are no more BitLocker recovery options on your PC" message and resembles the following screenshot:



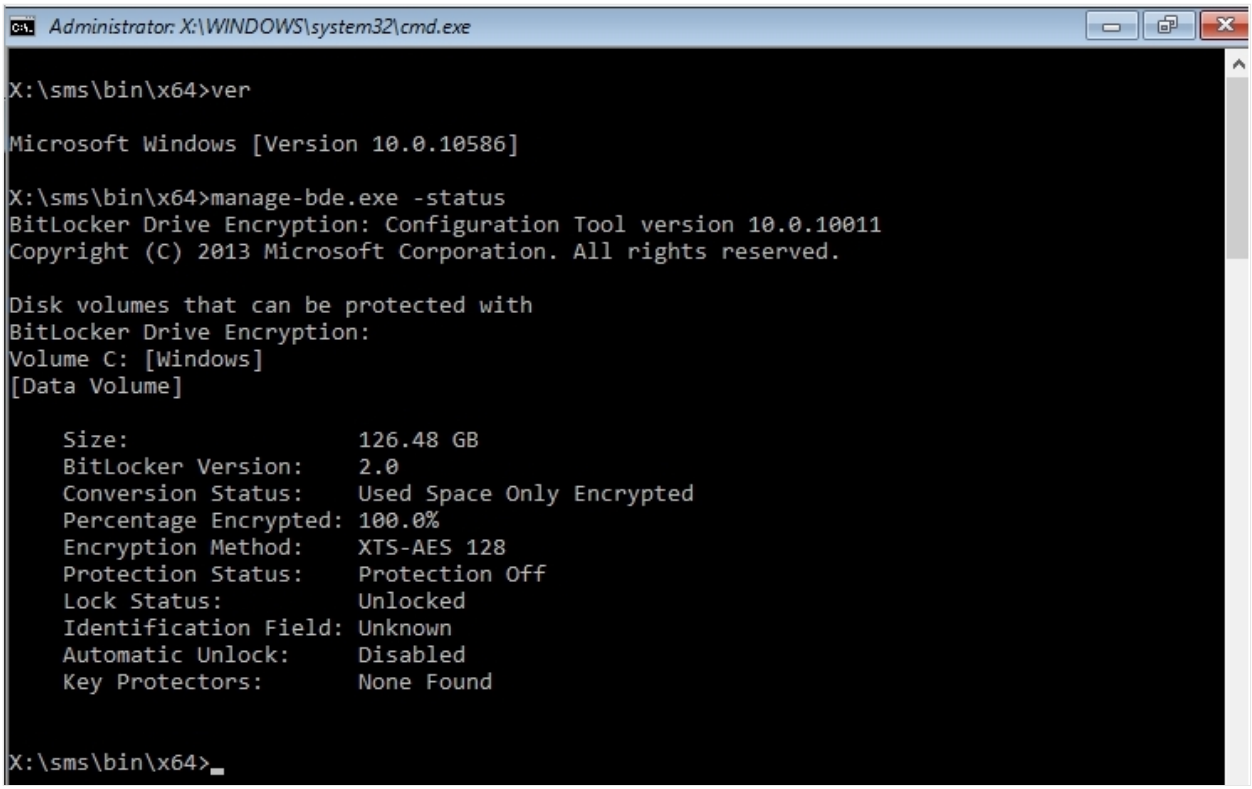
Cause

This problem occurs because the default encryption in Windows 10, version 1511 was changed from AES 128 to XTS-AES 128 to improve security. The new encryption method is not recognized by systems versions that were released before Windows 10, version 1511.

To verify this situation, enable command-line support, and run the following command during the Windows PE phase:

Console

```
manage-bde.exe -status
```

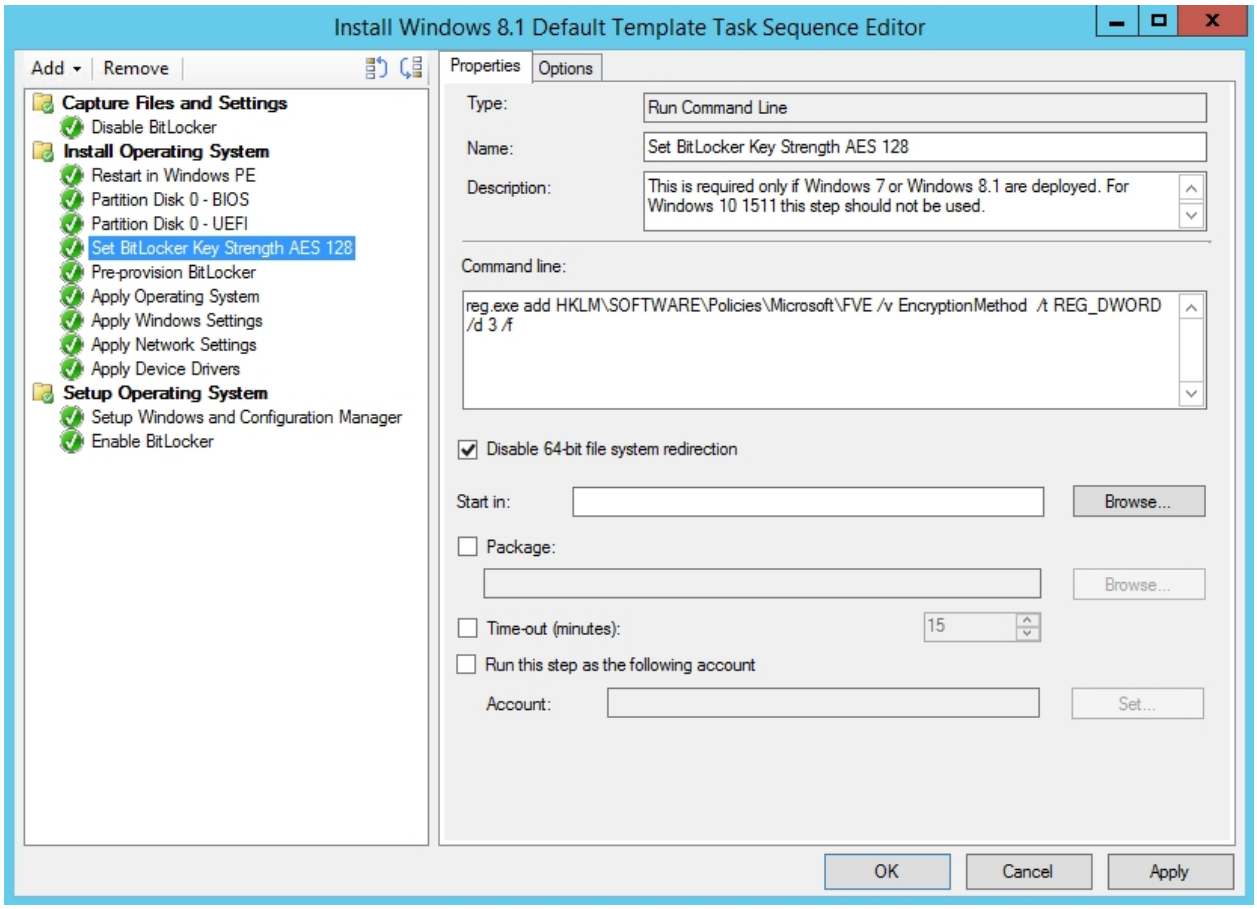


Resolution

To resolve this issue, use a **Run Command Line** step. To do this, add the following command before the "Pre-Provision BitLocker" task sequence step:

Console

```
reg.exe add HKLM\SOFTWARE\Policies\Microsoft\FVE /v EncryptionMethod  /t
REG_DWORD /d 3 /f
```



If an x64 boot image is used, select the option to disable 64-Bit file system redirection.

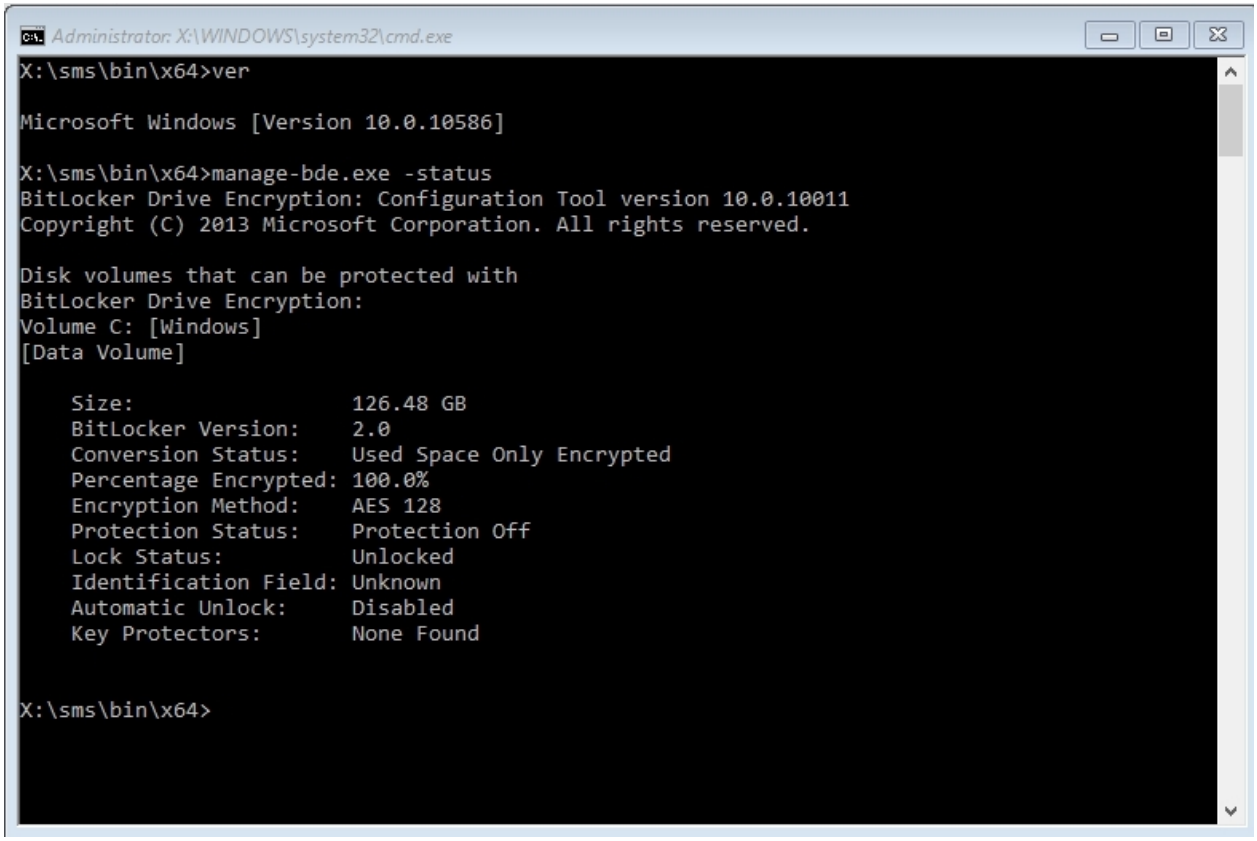
If you prefer other encryption methods, such as AES 256, use the guidance in the following table.

Value	Encryption method	Meaning and command line syntax
1	AES_128_WITH_DIFFUSER	The volume has been fully or partially encrypted by the Advanced Encryption Standard (AES) algorithm and enhanced by using a diffuser layer that has an AES key size of 128 bits. `reg.exe add HKLM\SOFTWARE\Policies\Microsoft\FVE /v EncryptionMethod /t REG_DWORD /d 1 /f`
2	AES_256_WITH_DIFFUSER	The volume has been fully or partially encrypted by the Advanced Encryption Standard (AES) algorithm and enhanced by using a diffuser layer that has an AES key size of 256 bits. `reg.exe add HKLM\SOFTWARE\Policies\Microsoft\FVE /v EncryptionMethod /t REG_DWORD /d 2 /f`

Value	Encryption method	Meaning and command line syntax
3	AES_128	The volume has been fully or partially encrypted by the Advanced Encryption Standard (AES) algorithm that has an AES key size of 128 bits. `reg.exe add HKLM\SOFTWARE\Policies\Microsoft\FVE /v EncryptionMethod /t REG_DWORD /d 3 /f`
4	AES_256	The volume has been fully or partially encrypted by the Advanced Encryption Standard (AES) algorithm that has an AES key size of 256 bits. `reg.exe add HKLM\SOFTWARE\Policies\Microsoft\FVE /v EncryptionMethod /t REG_DWORD /d 4 /f`
6	XTS_AES128 *	The volume has been fully or partially encrypted by the Advanced Encryption Standard (AES) algorithm that has an XTS-AES key size of 128 bits. This is the default for Windows PE 10.0.586.0 (version 1511). `reg.exe add HKLM\SOFTWARE\Policies\Microsoft\FVE /v EncryptionMethod /t REG_DWORD /d 6 /f`
7	XTS_AES256 *	The volume has been fully or partially encrypted by the Advanced Encryption Standard (AES) algorithm that has an XTS-AES key size of 256 bits. `reg.exe add HKLM\SOFTWARE\Policies\Microsoft\FVE /v EncryptionMethod /t REG_DWORD /d 7 /f`

* Supported for deployments of Windows 10 images, version 1511, or later versions only

Your system deployment will now work. The encryption method is again set to AES 128, as it was in older Windows PE releases.



References

What's new in Windows 10, versions 1507 and 1511

TPM is in reduced functionality mode after successful deployment of Windows 10

Article • 09/23/2021 • 2 minutes to read

This article provides a workaround for an issue in which the Trusted Platform Module (TPM) is in reduced functionality mode after a successful deployment of Windows 10.

Applies to: Windows 10 – all editions
Original KB number: 4018657

Symptoms

Consider the following scenario:

- You use Microsoft Deployment Toolkit (MDT) to deploy Windows 10. (This can be any version of MDT that supports Windows 10.)
- You use the "Enable BitLocker (offline)" step (ZTIBDE.wsf script) to pre-provision BitLocker during Windows PE in the "Preinstall" group.
- The deployment is successful.

In this scenario, you notice that the Trusted Platform Module (TPM) is in reduced functionality mode. In this situation, the TPM Management console (TPM.msc) reports the following issue:

> The TPM is ready for use, with reduced functionality. Information Flags: 0x900
> The TPM owner authorization is not properly stored in the registry.
> Windows's registry information about the TPM's Storage Root Key does not match the TPM Storage Root Key or is missing.

Cause

This issue occurs because the **TpmValidate** function in the ZTIBDE.wsf script takes ownership of the TPM from Windows PE unnecessarily. Windows should be able to correctly take ownership of the TPM before OOBE to provision it by using the correct parameters.

When this change in ownership of the TPM from Windows PE occurs, the TPM is given parameters that Windows doesn't understand. Therefore, the key hierarchies in the TPM

are disabled and made permanently unavailable to Windows.

Workaround

To work around this issue for new deployments until a new version of MDT is available, add the following command to the ZTIBDE.wsf script at the start of the "Function Main" section:

Console

```
reg add hklm\system\currentcontrolset\services\tpm\wmi -v
UseNullDerivedOwnerAuth -t REG_DWORD -d 0x01 -f
```

> **Note**
>
> For devices in which the TPM is already in reduced functionality mode, the TPM must be cleared before you can mitigate this issue. We recommend that you reset the TPM if it's in this state. To do this, follow the recommendations in **Clear all the keys from the TPM**.

More information

One option to prevent this issue from occurring isn't to pre-provision BitLocker, and to wait to enable the full system, instead. Be aware that the deployment will take longer to complete by using this method.

Windows 10 BitLocker Recovery auto-shutdown in UEFI mode

Article • 09/23/2021 • 2 minutes to read

This article discusses a by-design behavior where a computer shuts down after the BitLocker Drive Encryption Recovery screen is displayed for one minute. The one-minute shutdown occurs when the system is in Unified Extensible Firmware Interface (UEFI) mode.

Applies to: Windows 10 - all editions
Original KB number: 3174095

Symptoms

A computer shuts down after the BitLocker Drive Encryption Recovery screen is displayed for one minute.

Consider the following scenario:

- You configure the system for Unified Extensible Firmware Interface (UEFI) mode.
- You turn on BitLocker Drive Encryption for the boot (system) partition on drive C.
- You disable the Trusted Platform Module (TPM) chip or you change the boot files so that the BitLocker Drive Encryption Recovery screen is displayed on restart.
- You restart the computer to the BitLocker Drive Encryption Recovery screen.
- You do not touch the BitLocker Drive Encryption Recovery screen for one minute. Then, the computer shuts down.

Cause

This behavior is by design. We added this shutdown event to the system, and set it to occur after 60 seconds.

More information

The one-minute shutdown occurs when the system is in UEFI mode. The behavior is different when the system is set up in BIOS mode. Systems that are configured for BIOS mode do not shut down in this manner.

> ⓘ **Note**

BIOS mode is also known as legacy mode and compatibility mode.

BitLocker could not be enabled when USB drive is not found

Article • 12/06/2021 • 2 minutes to read

This article provides a resolution to an issue where BitLocker could not be enabled when USB drive isn't found.

Applies to: Windows Server 2012 R2, Windows 7 Service Pack 1
Original KB number: 2732377

Symptoms

When attempting to turn on BitLocker using a Startup Key as a protector and the system check option is accepted, BitLocker restarts the machine to complete the hardware test. If the USB drive holding the Startup Key is removed, or if USB ports are not enumerated correctly by the BIOS, then BitLocker isn't enabled on the volume and you may see following error message:

> BitLocker could not be enabled.
> The BitLocker encryption key cannot be obtained. Verify that the Trusted Platform Module (TPM) is enabled and ownership has been taken. If this computer does not have a TPM, verify that the USB drive is inserted and available.
> C: was not encrypted.



Cause

Boot Manager (Bootmgr) verifies that, the key material needed to unlock the disk is available before booting and starting encryption. If it is not available during the pre-boot hardware test before encryption, BitLocker will refuse to encrypt rather than leave the disk in a state that may not be usable in the expected manner. In the Startup Key case, this can occur when Bootmgr fails to find the Startup Key, either because then USB flash drive containing the Startup Key wasn't plugged in, or because the BIOS did not correctly enumerate the USB port with the USB drive inserted.

Resolution

The resolution will depend on the underlying cause. If you have already verified that the USB flash drive containing the Startup Key is inserted correctly and securely in the USB port, try the following steps:

1. Some USB ports are not enumerated during boot. Try a different USB port.
2. Some USB drives cannot be read during boot. Try a different USB dongle.
3. Boot into the BIOS and ensure USB is supported at boot time.
4. Check to see if there is a firmware update for your machine.

Users cannot retrieve BitLocker Recovery key using MBAM 2.0 Self Service Portal

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an error that occurs when you try to open MBAM 2.0 Self Service Portal web page to retrieve BitLocker Recovery Key.

Applies to: Windows Server 2012 R2
Original KB number: 2870849

Symptoms

If a user attempts to open MBAM 2.0 Self Service Portal web page to retrieve BitLocker Recovery Key, the web page may fail to open. Additionally, you may receive the following error message:

> There was error contacting the MBAM database. Please try again later.

Cause

This problem can occur for two possible reasons:

1. Windows Firewall is blocking the traffic from machine to SQL Server.

   You will also see the below error message in the application logs where SSP feature is installed.

   > Exception message: A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)

2. User Support Service web.config file does not have connection string information.

Resolution

To resolve this problem, do the following:

For Windows Firewall issue:

Open firewall ports for SQL Server. By default SQL uses port 1433 if you have configured SQL with a default instance.

Configuring the Windows Firewall to Allow SQL Server Access

For User Support Service web.config file issue, follow the steps:

1. Connect to Server where MBAM 2.0 Self Service Portal feature is installed.
2. Open Windows Explorer and browse to c:\inetpub\MicrosoftBitLockerManagementSolution\UserSupportService directory.
3. Make a copy of web.config file.
4. Edit the web.config file and make sure the connection string information is correct as shown below.
5. In the <connectionStrings> block:

```
XML

<add name="ComplianceStatusConnectionString"
providerName="System.Data.SqlClient" connectionString=""/>
```

should be:

```
XML

<add name="ComplianceStatusConnectionString"
providerName="System.Data.SqlClient" connectionString=" Data Source=
[SQL server name];Initial Catalog=&quot;MBAM Compliance
Status&quot;;Integrated Security=SSPI;"/>
```

> ⓘ **Note**
>
> - Replace *[SQL server name]* with your SQL Server Name.
> - Replace *MBAM Compliance Status* with name of MBAM Compliance Status DB.

For example, if the name of your SQL Server is MBAMSQL and the name of MBAM Compliance DB is MBAM_Comp_DB, then the query should be:

XML

```
<add name="ComplianceStatusConnectionString"
providerName="System.Data.SqlClient" connectionString="*Data Source=
[MBAMSQL];Initial Catalog=&quot;MBAM_ Comp_DB &quot;;Integrated
Security=SSPI;*"/>
```

6. Save the web.config file.
7. Restart IIS Services on Server.
8. Now user should be to retrieve BitLocker Recovery key successfully from MBAM SSP webpage.

References

How to Use the Self-Service Portal to Regain Access to a Computer

Disk partition requirement for using Windows RE tools on a UEFI-based computer

Article • 09/23/2021 • 2 minutes to read

This article discusses the disk partition requirements for using Windows Recovery Environment (RE) tools on a Unified Extensible Firmware Interface (UEFI) computer.

Applies to: Windows 10 – all editions, Windows Server 2012 R2
Original KB number: 3135522

More information

The disk partition for Windows RE tools must be at least 300 MB. Typically, between 250-300 MB is allocated for the Windows RE tools image (Winre.wim), depending on base language and added customizations.

The allocation for Windows RE must also include sufficient free space for backup utilities to capture the partition. Follow these guidelines to create the partition:

- If the partition is smaller than 500 MB, it must have at least 50 MB of free space.
- If the partition is 500 MB or larger, it must have at least 320 MB of free space.
- If the partition is larger than 1 GB, it must have at least 1 GB free of free space.
- This partition must use the following Type ID:

  DE94BBA4-06D1-4D40-A16A-BFD50179D6AC

- The Windows RE tools should be in a partition that's separate from the Windows partition. This separation supports automatic failover and the startup of partitions that are encrypted by using Windows BitLocker Drive Encryption.

> **Important**
>
> If Windows RE doesn't work as expected, double the specified free space for the partition. For example, if your partition is less than 500 MB and has 50 MB of free space, increase the free space to 100 MB.

Error after you enter a BitLocker PIN at Windows startup: Too many PIN entry attempts

Article • 09/23/2021 • 2 minutes to read

This article helps fix an error (Too many PIN entry attempts) that occurs after you enter a BitLocker PIN at Windows startup.

Applies to: Windows 10 version 1809 and later versions, Windows Server 2012 R2, Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
Original KB number: 4009797

Symptoms

After you enter a BitLocker PIN at Windows startup on a new computer that is running an OEM version of Windows, you receive the following error message:

> Too many PIN entry attempts

Cause

This issue occurs because the OEM doesn't reset the lockout count before shipping the device.

Workaround

To work around this issue, try the following methods, in no particular order:

- Input the BitLocker recovery key.
- Wait until the unlock period expires, and then enter the correct PIN.
- Reinstall the operating system, and then reset the TPM chip.
- Unlock the drive or turn off BitLocker. To do it, follow these steps:

    1. At the BitLocker entry screen, press ESC to access other recovery options.
    2. Select the command prompt option.

3. Enter `Manage-bde` to either unlock the system drive or turn off BitLocker. To do it, enter the appropriate command, and then press Enter:

   Unlock the system drive:

```
Console

manage-bde -unlock <DriveLetter>: -recoverypassword <Password>
manage-bde -unlock <DriveLetter>: -recoverykey <RecoveryKey>
```

   Turn off BitLocker:

```
Console

manage-bde -off <DriveLetter>:
```

   For more information, see the following articles:
   - Manage-bde: unlock
   - Manage-bde: off

- Contact the OEM for support.

More information

For more information about how to reset the TPM chip, see Reset the TPM Lockout.

"TPM is ready for use, with reduced functionality" message when the BIOS is in legacy mode with TPM 2.0

Article • 09/23/2021 • 2 minutes to read

This article helps fix an error that occurs when you have the operating system installed in Legacy MBR mode (PC/AT) with Trusted Platform Module (TPM) version 2.0.

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2
Original KB number: 3123365

Symptoms

On a Windows Server-based operating system, you have the operating system installed in Legacy MBR mode (PC/AT) with Trusted Platform Module (TPM) version 2.0. In this situation, you receive a message in the TPM user interface stating that "The TPM is ready for use, with reduced functionality."

Resolution

On the operating systems that are listed in the Applies To section, TPM 2.0 is supported in UEFI mode only.

More information

TPM 2.0 is designed to be fully functional in UEFI mode. Systems must be in UEFI mode with TPM enabled and secure boot configured and enabled in order to attain the security status that's described in the following TechNet article:

Secure the Windows 8.1 boot process

For more information about secure boot and TPM, see the following resources:

Windows hardware certification requirements for Client and Server systems

Trusted computing group

Third-party contact disclaimer

Microsoft provides third-party contact information to help you find additional information about this topic. This contact information may change without notice. Microsoft does not guarantee the accuracy of third-party contact information.

Event ID 15 may be logged when a Windows-based computer that has a TPM chip resumes from sleep

Article • 09/23/2021 • 2 minutes to read

This article describes a problem that may occur when a computer that has a Trusted Platform Module (TPM) chip resumes from sleep.

Applies to: Windows Server 2012 R2, Windows 7 Service Pack 1, Windows Server 2008 R2 Service Pack 1
Original KB number: 2696920

Symptoms

Consider the following scenario:

- You use a Trusted Platform Module (TPM) chip on a computer that is running Windows 8.1, Windows Server 2012 R2, Windows 8, Windows Server 2012, Windows 7 or Windows Server 2008 R2.
- You put the computer to sleep, and then you resume the computer from sleep.

In this scenario, the following event may be logged in the System log:

> The TPM driver and the TPM Base Services (TBS) log these errors when they cannot obtain a random number from the TPM chip for the Windows operating system. The operating system uses this random number as an additional source of entropy when the operating system's cryptographic methods generate random numbers.

Cause

When the TPM chip resumes from sleep, it must receive a command to continue a self-test before it is ready to process other commands. On many computers, the system BIOS will issue a command to the TPM chip to continue the self-test. If Windows tries to retrieve a random number while this self-test is being processed, the command fails with `TPM_DOING_SELFTEST`. When Windows receives this error, it retries up to three times. If the command continues to fail, the operating system logs the event that is mentioned in the "Symptoms" section and then moves on.

More information

You can safely ignore these errors, because Windows will fall back to the same mechanisms that are used to generate random numbers on systems that do not have a TPM chip. Additionally, Windows periodically retrieves a random number from the TPM chip. If this event is logged only one time, operating system was able to successfully obtain a random number.

References

For information about the TPM specification, see the Trusted Computing Group (TCG) TPM Specification, Version 1.2, and the TCG PC Client TPM Interface Specification, Version 1.2. To do this, visit the following Trusted Computing Group website: http://www.trustedcomputinggroup.org/developers/pc_client/specifications

Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft does not guarantee the accuracy of this third-party contact information.

The third-party products that this article discusses are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, about the performance or reliability of these products.

How to enable BitLocker device encryption on Windows 8 RT

Article • 12/06/2021 • 3 minutes to read

This document describes the workflow to enable BitLocker device encryption on the local hard disk of a Windows Surface computer that is running Windows 8 RT.

Applies to: Windows 8
Original KB number: 2855131

Summary

The document makes the following points:

- Logons by guest accounts, local administrator accounts, or Microsoft accounts that are members of the guest group don't trigger BitLocker encryption of the local hard disk.
- The first logon by a Microsoft account that is a member of the local computer's Administrators security group triggers BitLocker encryption of the local hard disk. A restart is required to complete the feature configuration.
- The BitLocker recovery password is put on the OneDrive share of the administrator-enabled Microsoft account that triggered the encryption. That recovery key isn't visible on the OneDrive share when the share is viewed by using a web browser or a OneDrive viewing application.
- Windows Explorer displays a padlock next to local drives that are BitLocker encrypted.
- BitLocker recovery keys may be obtained from the following website through an email message, a telephone call, or a text message:
  Find my BitLocker recovery key

More information

> **Note**
>
> The sizes of dialog boxes and other UI elements that are depicted in this article were changed. Changes include the placement of text in a dialog box and the size/aspect ratio.

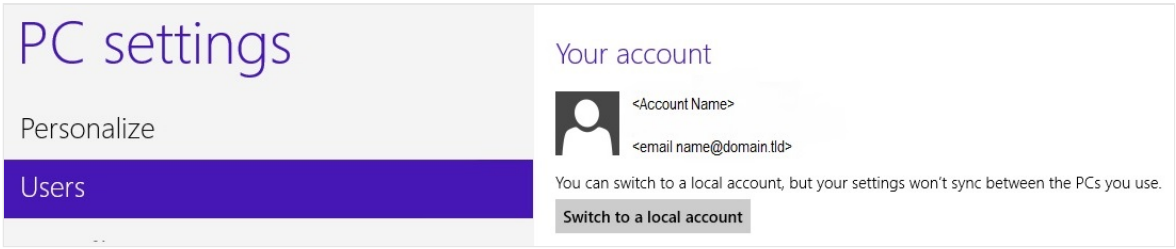
To see how the BitLocker device encryption workflow works, follow these steps:

1. On a new Windows 8 RT-based system, create a Guest account, and then log on by using that account.

2. Check the BitLocker status in Control Panel. The Guest user can't invoke BitLocker encryption.



3. Create a Microsoft account, and then associate that account with the Guest account that you created in step 1.



4. Log off.

5. Log on by using the Microsoft account that you created in step 3. Notice that the BitLocker add-in reports that the drive isn't protected.

6. Restart the computer, and then log on again by using the Microsoft account that you created in step 3. Notice that the BitLocker protection status remains unchanged.

   The net result is that logons that were made by using Microsoft accounts that are members of the Guest group don't trigger BitLocker encryption of the hard disk.

7. Create a new local account that is a member of the local computer's Administrators security group. Notice that the BitLocker add-in reports that the drive isn't protected.

8. Restart the computer. Again, notice that the BitLocker add-in reports that the drive isn't protected.

   The net result is that user logons that were made by using local computer accounts that are members of the Administrators group don't trigger BitLocker

encryption of the hard disk.

9. Associate the administrator account that you created in step 7 with a new Microsoft account.

10. Log on by using the Microsoft account that now has administrator permissions. Notice the following on-screen message:

    > Configuring Windows Feature
    > X % computer
    > Do not turn off your computer

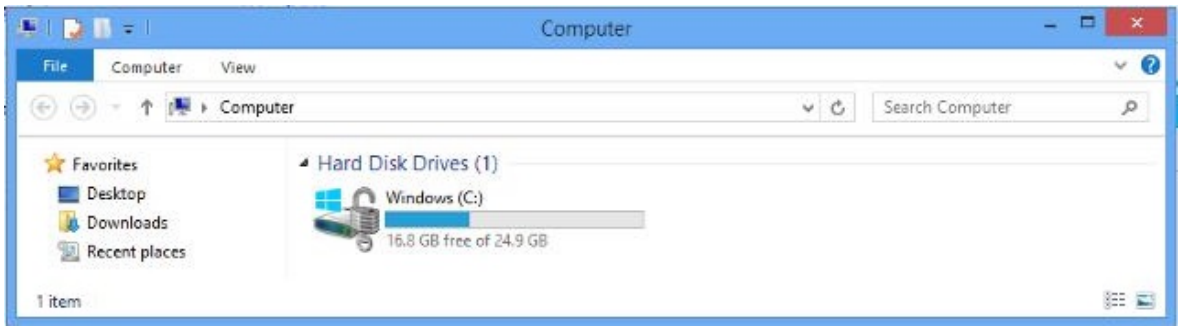
11. Restart the computer when you're prompted, and notice that the "Configuring Windows Feature" operation continues.

    The net result is that the first logon by a Microsoft account that is a member of the local computer's Administrators group triggers BitLocker encryption of the local drive.

12. Log on by using the Microsoft account that is a member of the Administrators group that you originally created in step 7. Notice the text change that is displayed by the BitLocker item in Control Panel.

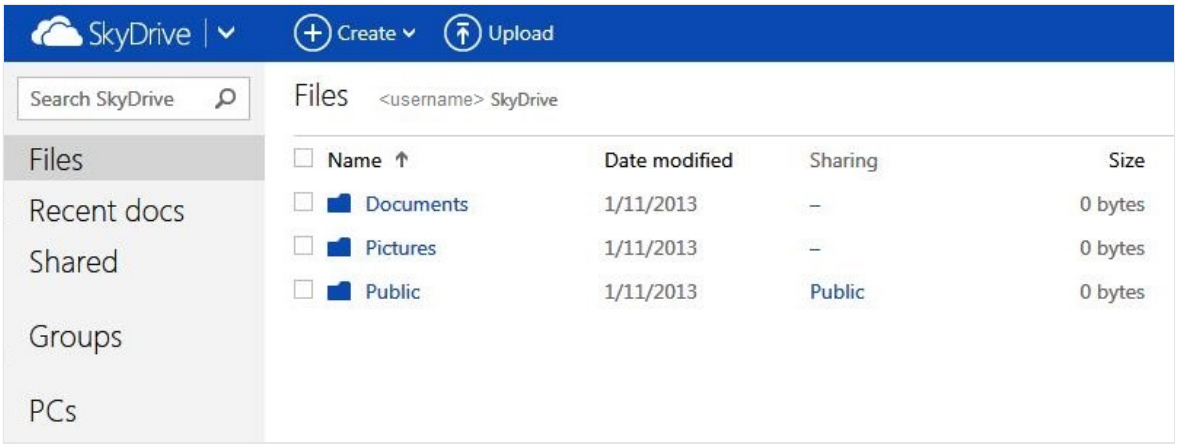


13. The padlock icon in Windows Explorer reports that the local drive is BitLocker protected.



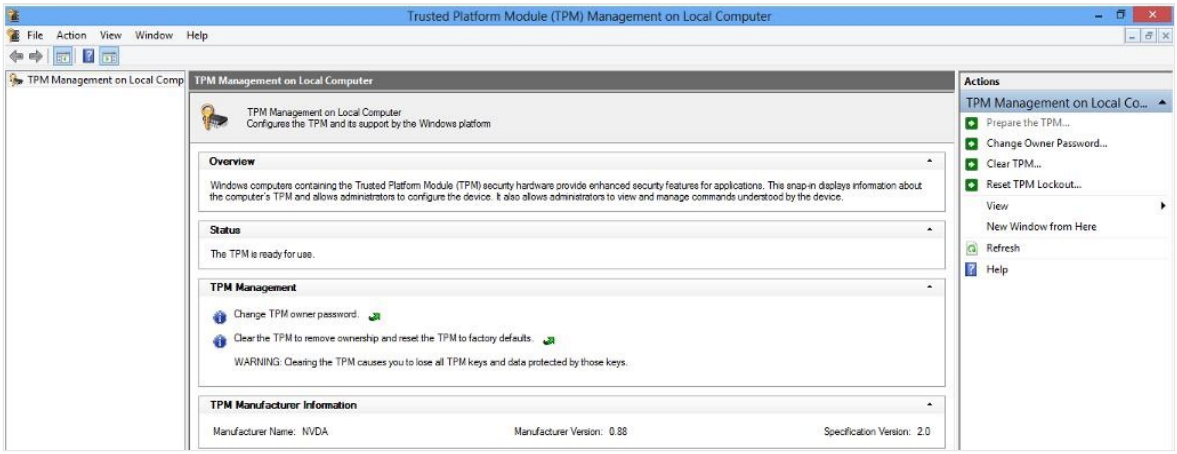
14. Notice that OneDrive never identifies the BitLocker recovery key.

Even after the local drive is clearly BitLocker encrypted and the Control Panel UI says that the BitLocker recovery key is stored on the first logon of a Microsoft account that is a member of the local computer's administrative group, OneDrive doesn't show any BitLocker-related files.

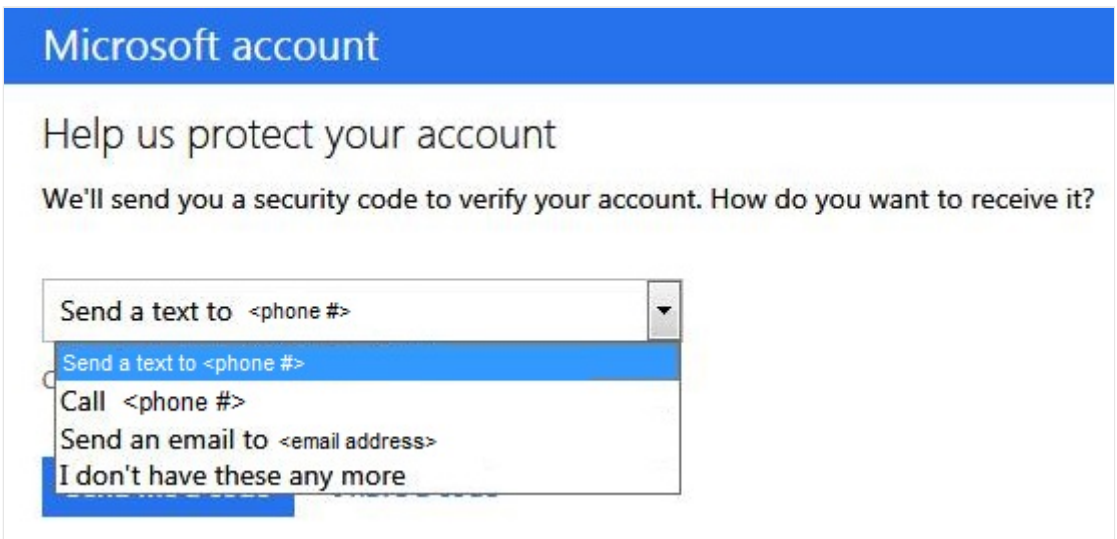


The net result is that the OneDrive share for the administrator-enabled Microsoft account that triggered the BitLocker device encryption shows no files.

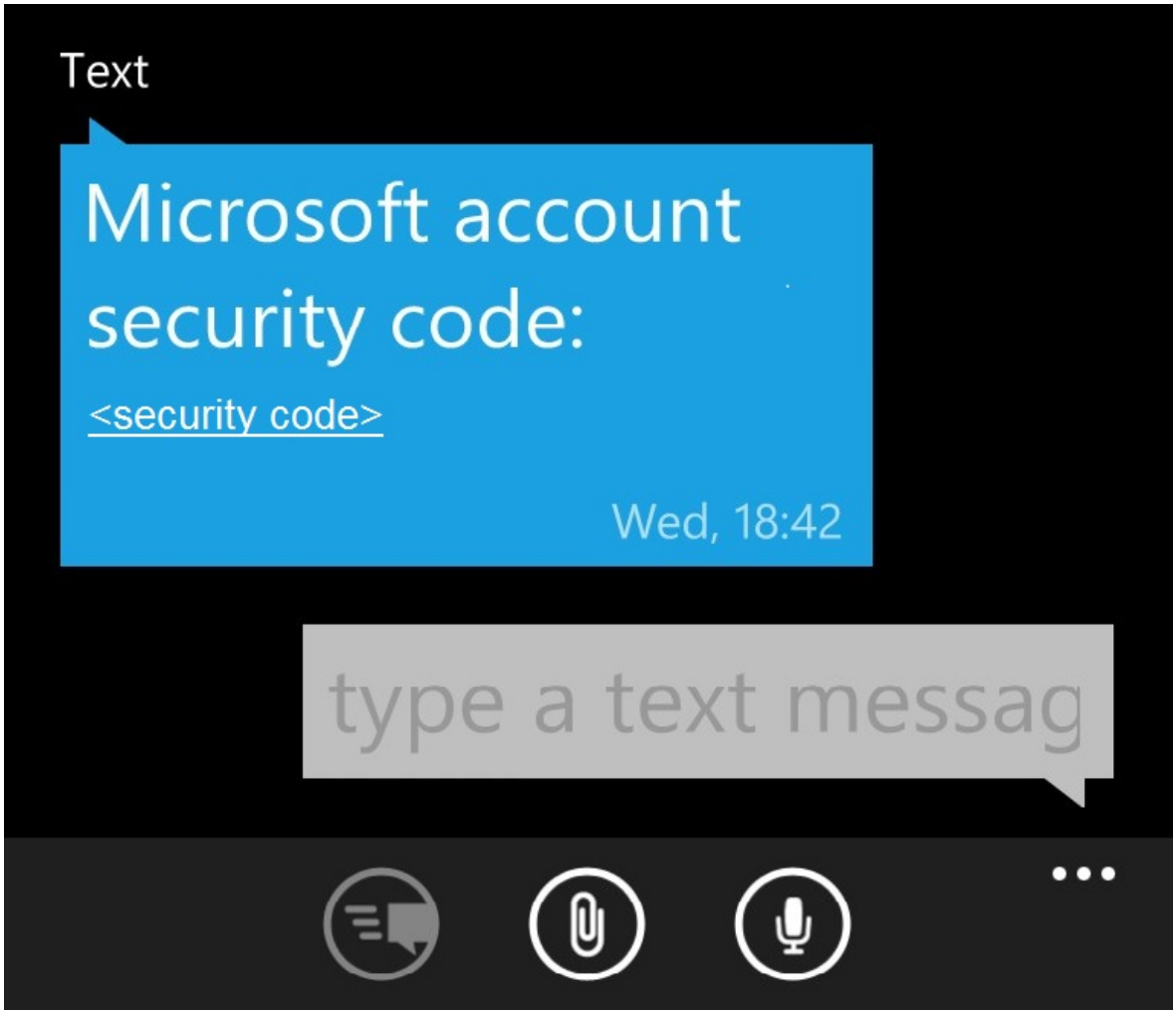
15. Notice that the TPM.MSC snap-in displays a status of "The TPM is ready for use."



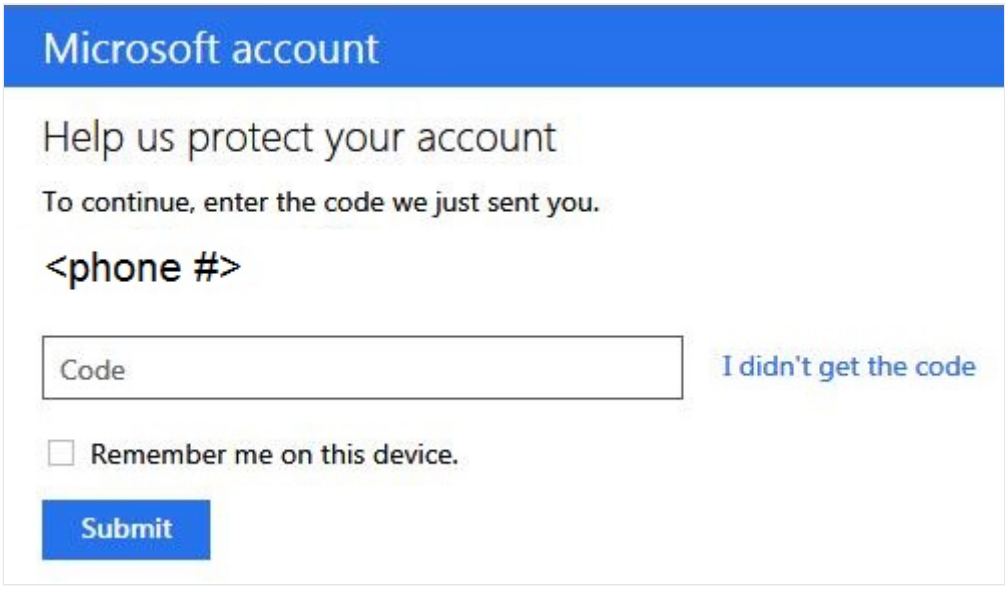
16. Connect to Find my BitLocker recovery key. You see the following options:



17. If you sent the recovery key by using a text message, the targeted phone will receive a text message that contains the Microsoft account security code. The text message resembles the following:



18. Type the code that you received in the text message into the Find my BitLocker recovery key wizard.



The Find my BitLocker recovery key wizard reports the BitLocker recovery key.


Microsoft account
BitLocker recovery keys
<computer name>
Key ID: <key id>
Recovery key: <8 octet recovery key>
Not finding the key you need? Learn more

MBAM client would fail with Event ID 4 and error code 0x8004100E in the Event description

Article • 09/23/2021 • 2 minutes to read

This article helps fix the error 0x8004100E that occurs when Microsoft BitLocker Administration and Monitoring (MBAM) client fails.

Applies to: Windows 7 Service Pack 1
Original KB number: 2756402

Symptoms

When an MBAM agent running on Windows 7 computer tries to communicate to MBAM server, it may fail to send the encryption status data. Additionally, you may receive the following event error message logged in the Event Viewer:

> Log Name: Microsoft-Windows-MBAM/Admin
> Source: Microsoft-Windows-MBAM
> Event ID: 4
> Task Category: None
> Level: Error
> Keywords:
> User: SYSTEM
> Computer: `<computername.domain.com>`
> Description: An error occurred while sending encryption status data. Error code: 0x8004100e

> **Note**
>
> Error code 0x8004100e translates to WBEM_E_INVALID_NAMESPACE.

Cause

This problem occurs if the BitLocker WMI class (win32_encryptablevolume) is not registered or missing registration.

Resolution

To resolve this problem, re-register the BitLocker WMI (win32_encryptablevolume) class.

Open an elevated command prompt and type the following command:

```
mofcomp.exe c:\windows\system32\wbem\win32_encryptablevolume.mof
```

If the file successfully compiles, you will receive the following message:

> Microsoft (R) MOF Compiler Version 6.1.7600.16385
> Copyright (c) Microsoft Corp. 1997-2006. All rights reserved.
> Parsing MOF file: win32_encryptablevolume.mof
> MOF file has been successfully parsed
> Storing data in the repository...
> Done!

MBAM can now send encryption status data to MBAM Compliance Database on SQL Server.

More information

To view MBAM event logs on a Windows 7 client machine browse to:

1. Click the Start button, type "event viewer" in search box, then click on Event Viewer that will be displayed above.
2. Click on Application and Services Logs
3. Select Microsoft
4. Expand Windows
5. Expand MBAM and then select Admin Logs.

ⓘ Note

BitLocker WMI Provider interface, for example Win32_EncryptableVolume WMI provider class is used to manage and configuring BitLocker Drive Encryption (BDE) on Windows Server 2008 R2, Windows Server 2008, and only specific versions of Windows 7, Windows Vista Enterprise, and Windows Vista Ultimate. MBAM client and manage-bde.exe command use this WMI class to administer and capture the current status of BDE on a volume. In case the namespace for this class is missing/corrupt, administrative tools including MBAM and manage-bde.exe will fail with errors. Additionally, you may get below error message if you run the manage-bde command:

Also, see following MSDN article for: Running the MOF Compiler on a File

Parameter is incorrect error message when you try to enable BitLocker if you don't have a separate active partition in Windows Server 2008 Core and Windows 2008 R2 Core Edition

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an error when you try to enable BitLocker if you don't have a separate active partition.

Applies to: Windows 7 Service Pack 1, Windows Server 2012 R2
Original KB number: 2019926

Symptoms

When you try to enable BitLocker drive encryption on the operating system drive (typically drive C) by using the `manage-bde.exe -on` command, you may receive the following error message:

> ERROR: An error occurred <code 0x80070057>
> The parameter is incorrect

Cause

This problem occurs if you don't have a separate active system partition on the operating system drive.

Resolution

To resolve this issue, create a separate active system partition that can be used by BitLocker. The steps in this process vary, depending on the operating system that you're using and on whether you're using the `manage-bde` command or the BitLocker setup wizard.

Assume that you're upgrading from an earlier version of Windows or that you're installing Windows 7 or Windows Server 2008 R2 on a new computer that has a single

partition. When you enable BitLocker from Control Panel or from Windows Explorer in this situation, the BitLocker setup wizard automatically configures the target drive for the separate active system partition. However, in some rare instances, you may have to manually prepare the drive for BitLocker. In this situation, use one of the following methods, as appropriate for your operating system.

Windows Server 2008 or Windows Vista:

Use the BitLocker Drive Preparation tool that is discussed in Description of the BitLocker Drive Preparation Tool to create a separate active system partition that can be used by BitLocker.

Windows 2008 Core or Windows Server 2008 R2 with BitLocker feature installed:

Use the BitLocker Drive Preparation tool to create a separate active system partition that can be used by BitLocker. You can find this tool in the `C:\Windows\System32` directory.

Use the following `bdehdcg.exe` command line to create a system partition for BitLocker: **bdehdcfg -target c: shrink -newdriveletter s: -size 300**

> ⓘ Note
>
> In this command line, "c" represents the operating system drive, "s" represents the drive letter for the new system partition, and "300" represents the size of the partition in megabytes (MB).

You must restart the computer to complete this operation.

> ⓘ Note
>
> The Bdehdcfg.exe utility not available in Windows Server 2008 R2 Core. To use this utility in Windows Server 2008 R2 Core, copy the following three files from the `C:\Windows\System32` directory of a computer that is running Windows 2008 R2 Enterprise, Windows 2008 R2 Standard, or Windows 2008 R2 Web Full Edition to the `C:\Windows\System32` directory of the Windows 2008 R2 2008 R2 Core-based computer that is generating the error:
>
> - Bdehdcfg.exe
> - Bdehdcfglib.dll
> - Reagent.dll

More information

- Enabling BitLocker by Using the Command Line
- Using the BitLocker Drive Preparation Tool for Windows 7

Error when you enable BitLocker: The specified account does not exist

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution to an error (the specified account doesn't exist) that occurs when you try to enable BitLocker.

Applies to: Windows Server 2012 R2, Windows Server 2008 R2 Service Pack 1, Windows 7 Service Pack 1
Original KB number: 2665635

Symptoms

When a new user logs in to a machine and attempts to enable BitLocker, the following error occurs:

> The specified account does not exist.

Cause

When the current user account isn't recognized by the AD, BitLocker receives a standard error code - ERROR_NO_SUCH_USER, which is converted to the standard error message: The specified account does not exist.

One reason this error message can be thrown is, if the BitLocker wizard failed to back up the recovery password to Active Directory because the account is not fully replicated to all domain controllers, in particular the one the client connected to.

Resolution

Wait for AD replication to complete for the account and try again.

Suspend BitLocker protection for non-Microsoft software updates

Article • 11/22/2021 • 2 minutes to read

Applies to: Windows 10

You must temporarily disable BitLocker protection by using the **Suspend protection** feature for non-Microsoft software updates such as:

- Computer manufacturer firmware updates
- TPM firmware updates
- Non-Microsoft application updates that modify boot components

> **Important**
>
> If BitLocker protection isn't suspended, the system won't recognize the BitLocker key and you'll be prompted to enter the recovery key to proceed next time the system restarts. Not having a recovery key will cause data loss or an unnecessary operating system reinstallation. This will happen every time you restart the system.

Suspending BitLocker protection on a system drive prevents certain problems and allows successful firmware and hardware updates. You can suspend BitLocker protection and resume it at any time by using the **Control Panel** or **PowerShell**.

> **Note**
>
> BitLocker protection will remain disabled for a particular drive until you manually resume it.

Suspend and resume BitLocker protection by using the Control Panel

Here's how to suspend BitLocker protection:

1. Open **Control Panel**.
2. Select **System and Security** > **BitLocker Drive Encryption** > **Suspend protection**.
3. Select **Yes**.

Here's how to resume BitLocker protection:

1. Open **Control Panel**.
2. Select **System and Security** > **BitLocker Drive Encryption** > **Resume protection**.
3. Select **Yes**.

Suspend and resume BitLocker protection by using PowerShell

Here's how to suspend BitLocker protection:

1. Go to Start.
2. Go to Search, enter the word *PowerShell*, press and hold (or right-click) **Windows PowerShell**, and then select **Run as administrator**.
3. In the **Administrator: Windows PowerShell** window, enter the following command and press Enter:

```
PowerShell
```

```
Suspend-BitLocker -MountPoint "C:" -RebootCount 0
```

> **Note**
>
> In this command, the -RebootCount allows you to determine how many times your computer can restart before BitLocker protection is automatically re-enabled. You can use values from 0 to 15. A value of 0 will suspend BitLocker protection until you resume the protection manually.

Here's how to resume BitLocker protection:

1. Go to Start.
2. Go to Search, enter the word *PowerShell*, press and hold (or right-click) **Windows PowerShell**, and then select **Run as administrator**.
3. In the **Administrator: Windows PowerShell** window, enter the following command and press Enter:

```
PowerShell
```

```
Resume-BitLocker -MountPoint "C:"
```

The encryption protection feature is now enabled on your device.

The recovery password for Windows BitLocker isn't available when FIPS compliant policy is set in Windows

Article • 11/17/2022 • 2 minutes to read

This article discusses the issues that occur because the recovery password for Windows BitLocker isn't FIPS-compliant in Windows.

Applies to: Windows 7 Service Pack 1, Windows Server 2008 R2
Original KB number: 947249

Introduction

The key derivation algorithm used with the recovery password for Windows BitLocker Drive Encryption isn't Federal Information Processing Standards (FIPS)-compliant in Windows. Therefore, you may encounter the following issues when the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** Group Policy setting is enabled.

Issue 1

When you manually add a recovery password at a command prompt, you receive the following error message:

> The numerical password was not added. The FIPS Group Policy setting on the computer prevents recovery password creation.

Issue 2

When you try to encrypt a drive on which BitLocker recovery passwords are required, you can't encrypt the drive as expected. Additionally, you receive the following error message:

> Cannot Encrypt Disk. Policy requires a password which is not allowed with the current security policy about use of FIPS algorithms.

Issue 3

When you encrypt a drive, a recovery key is created, but no recovery password is created as a key protector.

Issue 4

A recovery password isn't archived in the Active Directory directory service.

More information

A BitLocker recovery password has 48 digits. This password is used in a key derivation algorithm that isn't FIPS-compliant. Therefore, if you enable the System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing Group Policy setting, you can't create or unlock a drive by using a recovery password. In contrast, a BitLocker recovery key is an AES key that doesn't require a key derivation algorithm to be performed upon it and is FIPS-compliant. Therefore, a recovery key isn't affected by this Group Policy setting.

To disable the System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing Group Policy setting, follow these steps:

1. Click **Start**, type *gpedit.msc* in the **Start Search** box, and then click **OK**.

   > ⓘ **Note**
   >
   > If you are prompted for an administrator password or for confirmation, type the password, or provide confirmation.

2. Expand **Computer Configuration**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
3. In the details pane, double-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**, click **Disable**, and then, click **OK**.

> ⓘ **Note**
>
> This Group Policy setting may be configured by an administrator to be automatically applied from a domain controller. In this situation, you can't disable this setting locally.

MBAM 2.0 SSP Portal gives an error: The requested Key ID is invalid for the current user

Article • 09/23/2021 • 2 minutes to read

This article provides a solution to an error that occurs when you try to retrieve BitLocker Recovery Key using MBAM 2.0 Self Service Portal (SSP).

Applies to: Windows Server 2012 R2
Original KB number: 2870853

Summary

When a user tries to retrieve BitLocker Recovery Key using MBAM 2.0 Self Service Portal (SSP), it may give you the following error message:

> The requested Key ID is invalid for the current user.

More information

In MBAM 2.0, the Recovery Key ID is only shown to the user, if the user who is requesting the key has logged on to the machine at least once. Also, in MBAM 2.0, SQL database maintains the list of logon user after MBAM 2.0 agent is installed and always verifies if the user has logged in to the machine or not.

For example:

- User A logins to Computer A.
- Computer A asks for BitLocker Recovery Key due to some changes done on the machine.
- User A goes to Computer B and logins to Windows.
- Open MBAM 2.0 Self Service Portal (`https://mbamserver/selfservice`).
- Enter the first eight digits of recovery key ID and MBAM 2.0 SSP page will show the user the recovery key.
- Let's say if user A never logged in to computer A, then we won't show the user the key and will throw the above message.

"Not enough storage is available to complete this operation" error message when you use a domain controller to join a computer to a domain

Article • 09/23/2021 • 2 minutes to read

This article provides a resolution for the error "Not enough storage is available to complete this operation", when you use a domain controller to join a computer to a domain.

Applies to: Windows Server 2019, Windows Server 2016, Windows Server 2012 R2
Original KB number: 935744

Symptoms

When you use a Microsoft Windows Server 2003 or later version domain controller to join a Microsoft Windows XP or later version client computer to a domain, you may receive an error message that resembles the following on the client computer:

> The following error occurred attempting to join the domain "**domain_name.com**":
> Not enough storage is available to complete this operation.

Additionally, the following Warning message may be logged in the System log on the client computer:

Cause

This problem occurs because the Kerberos token that is generated during authentication is more than the fixed maximum size. In the original release version of Microsoft Windows 2000, the default value of the MaxTokenSize registry entry was 8,000 bytes. In Windows 2000 with Service Pack 2 (SP2) and in later versions of Windows, the default value of the MaxTokenSize registry entry is 12,000 bytes.

For example, if a user is a member of a group either directly or by membership in another group, the security ID (SID) for that group is added to the user's token. For a SID to be added to the user's token, the SID information must be communicated by

using the Kerberos token. If the required SID information exceeds the size of the token, authentication is unsuccessful.

Resolution

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:
> 322756 How to back up and restore the registry in Windows

To resolve this problem, increase the Kerberos token size. Follow these steps on the client computer that logs the Kerberos event.

1. Click **Start**, click **Run**, type regedit, and then click **OK**.
2. Locate and then click the following registry subkey:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters`

   > **Note**
   >
   > If the **Parameters** key is not present, create the key. To do this, follow these steps:
   >
   > a. Locate and then click the following registry subkey:
   > `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos`
   > b. On the **Edit** menu, point to **New**, and then click **Key**.
   > c. Type Parameters , and then press ENTER.

3. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
4. Type MaxTokenSize, and then press ENTER.
5. On the **Edit** menu, click **Modify**.
6. In the **Base** area, click **Decimal**, type 65535 in the **Value data** box, and then click **OK**.

> **Note**
>
> The default value for the MaxTokenSize registry entry is a decimal value of 12,000. We recommend that you set this registry entry value to a decimal value of 65,535. If you incorrectly set this registry entry value to a hexadecimal value of 65,535, Kerberos authentication operations may fail. Additionally, programs may return errors.

7. Exit Registry Editor.
8. Restart the computer.

More information

For more information, click the following article numbers to view the articles in the Microsoft Knowledge Base:

327825 New resolution for problems with Kerberos authentication when users belong to many groups

"File system error" when pasting password into credential dialog box in Windows 10

Article • 03/24/2022 • 2 minutes to read

This article provides help to fix a File system error that occurs when you paste password into a credential dialog box.

Applies to: Windows 10
Original KB number: 4092998

Symptoms

Consider the following scenario:

- You try to start an application by using elevated permissions. For example, you right-click cmd.exe and select **Run as administrator**.
- A User Account Control (UAC) dialog box prompts you for your user name and password.
- You press Ctrl+V to paste in the password.

In this scenario, you receive the following error messages:

> This program does not have a program associated with it for performing this action.

> File system error (-1073741189).

During investigation, you notice that Consent.exe crashes when the issue occurs. The error maps to the following information:

Code	Symbolic Name	Error Description	Header
Hex: 0xc000027b Dec: -1073741189	STATUS_STOWED_EXCEPTION	An application-internal exception has occurred.	ntstatus.h

Note

If you right-click the password box, a shortcut menu does not open.

Cause

Pasting the contents of the clipboard into a secure input box is intentionally blocked in Windows 10. However, the Consent.exe crash is a software problem.

Windows 10 introduces a security change that blocks clipboard access from the Winlogon desktop (also known as the secure desktop). This change prevents an unauthorized user from seeing information on the clipboard. For example, consider the following scenario:

- Authorized user A copies some information to the clipboard and then locks the computer.
- Unauthorized user B wakes up the computer (which is at the lock screen) and starts **Narrator -> Narrator Help**. From there, unauthorized user B can paste the clipboard contents into a text box in Narrator Help and then read the clipboard content.

A side effect of this change is that by default it is no longer possible to paste information into the password text box for UAC elevation.

Resolution

To fix the consent.exe crashing issue, install the Windows 10 cumulative update that was released on April 23, 2018 or later cumulative updates. For more information, see April 23, 2018-KB4093105 (OS Build 16299.402).

> **Note**
>
> This update only fixes the consent.exe crashing issue. Pasting password to secure input box is still blocked. If you want to paste the password to UAC, see the "Workaround" section.

Workaround

To work around this issue, display the UAC elevation prompt on the standard user desktop instead of on the Winlogon desktop. The UAC prompt behavior can be configured by using Group Policy. See User Account Control: Switch to the secure desktop when prompting for elevation for more information.

More information

Changing the desktop when UAC is displayed might raise security concerns. However, the copy/paste mechanism of moving the password from password vault software to a UAC prompt invalidates the security protection that is provided by the Winlogon desktop.

The reason why UAC prompts are displayed by default on the Winlogon desktop is that no nonsecure process (for example, one that is not already running as SYSTEM) can spy on passwords or other information that is input into the UAC dialog box. However, as soon as the password is copied and on the clipboard on the standard user desktop, any process that is running in that desktop can read that data in plain text. In effect, the potential security breach has already occurred with no need for any process to try to read the password information from a UAC dialog box.

Microsoft has verified that the security fix that is implemented in Windows 10 to enforce the correct security boundary from the standard desktop to the Winlogon desktop is the desired behavior, and this will likely remain the behavior in future versions of Windows.

Default encryption settings for the Microsoft L2TP/IPSec VPN Client

Article • 09/23/2021 • 2 minutes to read

This article describes the default encryption settings for the Microsoft L2TP/IPSec virtual private network (VPN) client.

Applies to: Windows 10 - all editions
Original KB number: 325158

Summary

The following list contains the default encryption settings for the Microsoft L2TP/IPSec virtual private network (VPN) client for earlier version clients:

- Data Encryption Standard
- Secure Hash Algorithm
- Diffie-hellman Medium
- Transport Mode
- Encapsulating Security Payload

The client does not support the following settings:

- Tunnel mode
- AH (Authentication Header)

These values are hard-coded in the client and you cannot change them.

Data Encryption Standard

Data Encryption Standard (3DES) provides confidentiality. 3DES is the most secure of the DES combinations, and has a bit slower performance. 3DES processes each block three times, using a unique key each time.

Secure Hash Algorithm

Secure Hash Algorithm 1 (SHA1), with a 160-bit key, provides data integrity.

Diffie-Hellman Medium

Diffie-Hellman groups determine the length of the base prime numbers that are used during the key exchange. The strength of any key derived depends in part on the strength of the Diffie-Hellman group on which the prime numbers are based.

Group 2 (medium) is stronger than Group 1 (low). Group 1 provides 768 bits of keying material, and Group 2 provides 1,024 bits. If mismatched groups are specified on each peer, negotiation does not succeed. You cannot switch the group during the negotiation.

A larger group results in more entropy and therefore a key that is harder to break.

Transport mode

There are two modes of operation for IPSec:

- Transport mode - In transport mode, only the payload of the message is encrypted.
- Tunnel mode (not supported) - In tunnel mode, the payload, the header, and the routing information are all encrypted.

IPSec Security Protocols

- Encapsulating Security Payload

  Encapsulating Security Payload (ESP) provides confidentiality, authentication, integrity, and anti-replay. ESP does not ordinarily sign the whole packet unless the packet is being tunneled. Ordinarily, only the data is protected, not the IP header. ESP does not provide integrity for the IP header (addressing).

- Authentication Header (not supported)

  Authentication Header (AH) provides authentication, integrity, and anti-replay for the whole packet (both the IP header and the data carried in the packet). AH signs the whole packet. It does not encrypt the data, so it does not provide confidentiality. You can read the data, but you cannot modify it. AH uses HMAC algorithms to sign the packet.

References

How to troubleshoot a Microsoft L2TP/IPSec virtual private network client connection

How to enable NTLM 2 authentication

Article • 09/23/2021 • 7 minutes to read

This article describes how to enable NTLM 2 authentication.

Applies to: Windows 10 - all editions
Original KB number: 239869

Summary

Historically, Windows NT supports two variants of challenge/response authentication for network logons:

- LAN Manager (LM) challenge/response
- Windows NT challenge/response (also known as NTLM version 1 challenge/response) The LM variant allows interoperability with the installed base of Windows 95, Windows 98, and Windows 98 Second Edition clients and servers. NTLM provides improved security for connections between Windows NT clients and servers. Windows NT also supports the NTLM session security mechanism that provides for message confidentiality (encryption) and integrity (signing).

Recent improvements in computer hardware and software algorithms have made these protocols vulnerable to widely published attacks for obtaining user passwords. In its ongoing efforts to deliver more secure products to its customers, Microsoft has developed an enhancement, called NTLM version 2, that significantly improves both the authentication and session security mechanisms. NTLM 2 has been available for Windows NT 4.0 since Service Pack 4 (SP4) was released, and it is supported natively in Windows 2000. You can add NTLM 2 support to Windows 98 by installing the Active Directory Client Extensions.

After you upgrade all computers that are based on Windows 95, Windows 98, Windows 98 Second Edition, and Windows NT 4.0, you can greatly improve your organization's security by configuring clients, servers, and domain controllers to use only NTLM 2 (not LM or NTLM).

More information

When you install Active Directory Client Extensions on a computer that is running Windows 98, the system files that provide NTLM 2 support are also automatically installed. These files are Secur32.dll, Msnp32.dll, Vredir.vxd, and Vnetsup.vxd. If you

remove Active Directory Client Extension, the NTLM 2 system files are not removed because the files provide both enhanced security functionality and security-related fixes.

By default, NTLM 2 session security encryption is restricted to a maximum key length of 56 bits. Optional support for 128-bit keys is automatically installed if the system satisfies United States export regulations. To enable 128-bit NTLM 2 session security support, you must install Microsoft Internet Explorer 4.x or 5 and upgrade to 128-bit secure connection support before you install the Active Directory Client Extension.

To verify your installation version:

1. Use Windows Explorer to locate the Secur32.dll file in the %SystemRoot%\System folder.
2. Right-click the file, and then click **Properties**.
3. Click the **Version** tab. The description for the 56-bit version is "Microsoft Win32 Security Services (Export Version)." The description for the 128-bit version is "Microsoft Win32 Security Services (US and Canada Only)."

Before you enable NTLM 2 authentication for Windows 98 clients, verify that all domain controllers for users who log on to your network from these clients are running Windows NT 4.0 Service Pack 4 or later. (The domain controllers can run Windows NT 4.0 Service Pack 6 if the client and server are joined to different domains.) No domain controller configuration is required to support NTLM 2. You must configure domain controllers only to disable support for NTLM 1 or LM authentication.

Enabling NTLM 2 for Windows 95, Windows 98, or Windows 98 Second Edition clients

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:
> 322756 How to back up and restore the registry in Windows

To enable a Windows 95, Windows 98, or Windows 98 Second Edition client for NTLM 2 authentication, install the Directory Services Client. To activate NTLM 2 on the client,

follow these steps:

1. Start Registry Editor (Regedit.exe).
2. Locate and click the following key in the registry:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control`
3. Create an LSA registry key in the registry key listed above.
4. On the Edit menu, click Add Value, and then add the following registry value:
   Value Name: LMCompatibility
   Data Type: REG_DWORD
   Value: 3
   Valid Range: 0,3
   Description: This parameter specifies the mode of authentication and session security to be used for network logons. It does not affect interactive logons.

   - Level 0 - Send LM and NTLM response; never use NTLM 2 session security. Clients will use LM and NTLM authentication, and never use NTLM 2 session security; domain controllers accept LM, NTLM, and NTLM 2 authentication.
   - Level 3 - Send NTLM 2 response only. Clients will use NTLM 2 authentication and use NTLM 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication.

   > ⓘ **Note**
   >
   > To enable NTLM 2 for Windows 95 Clients, install Distributed File System (DFS) Client, WinSock 2.0 Update, and Microsoft DUN 1.3 for Windows 2000.

5. Quit Registry Editor.

> ⓘ **Note**
>
> For Windows NT 4.0 and Windows 2000 the registry key is LMCompatibilityLevel, and for Windows 95 and Windows 98-based computers, the registery key is LMCompatibility.

For reference, the full range of values for the LMCompatibilityLevel value that are supported by Windows NT 4.0 and Windows 2000 include:

- Level 0 - Send LM and NTLM response; never use NTLM 2 session security. Clients use LM and NTLM authentication, and never use NTLM 2 session security; domain

controllers accept LM, NTLM, and NTLM 2 authentication.

- Level 1 - Use NTLM 2 session security if negotiated. Clients use LM and NTLM authentication, and use NTLM 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication.
- Level 2 - Send NTLM response only. Clients use only NTLM authentication, and use NTLM 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication.
- Level 3 - Send NTLM 2 response only. Clients use NTLM 2 authentication, and use NTLM 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication.
- Level 4 - Domain controllers refuse LM responses. Clients use NTLM authentication, and use NTLM 2 session security if the server supports it; domain controllers refuse LM authentication (that is, they accept NTLM and NTLM 2).
- Level 5 - Domain controllers refuse LM and NTLM responses (accept only NTLM 2). Clients use NTLM 2 authentication, use NTLM 2 session security if the server supports it; domain controllers refuse NTLM and LM authentication (they accept only NTLM 2).A client computer can only use one protocol in talking to all servers. You cannot configure it, for example, to use NTLM v2 to connect to Windows 2000-based servers and then to use NTLM to connect to other servers. This is by design.

You can configure the minimum security that is used for programs that use the NTLM Security Support Provider (SSP) by modifying the following registry key. These values are dependent on the LMCompatibilityLevel value:

1. Start Registry Editor (Regedit.exe).

2. Locate the following key in the registry:
   `HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\LSA\MSV1_0`

3. On the Edit menu, click Add Value, and then add the following registry value:
   Value Name: NtlmMinClientSec
   Data Type: REG_WORD
   Value: one of the values below:

   - 0x00000010- Message integrity
   - 0x00000020- Message confidentiality
   - 0x00080000- NTLM 2 session security
   - 0x20000000- 128-bit encryption
   - 0x80000000- 56-bit encryption

4. Quit Registry Editor.

If a client/server program uses the NTLM SSP (or uses secure Remote Procedure Call [RPC], which uses the NTLM SSP) to provide session security for a connection, the type of session security to use is determined as follows:

- The client requests any or all the following items: message integrity, message confidentiality, NTLM 2 session security, and 128-bit or 56-bit encryption.
- The server responds, indicating which items of the requested set it wants.
- The resulting set is said to have been "negotiated."

You can use the NtlmMinClientSec value to cause client/server connections to either negotiate a given quality of session security or not to succeed. However, you should note the following items:

- If you use 0x00000010 for the NtlmMinClientSec value, the connection does not succeed if message integrity is not negotiated.
- If you use 0x00000020 for the NtlmMinClientSec value, the connection does not succeed if message confidentiality is not negotiated.
- If you use 0x00080000 for the NtlmMinClientSec value, the connection does not succeed if NTLM 2 session security is not negotiated.
- If you use 0x20000000 for the NtlmMinClientSec value, the connection does not succeed if message confidentiality is in use but 128-bit encryption is not negotiated.

Enabling debug logging for the Netlogon service

Article • 09/23/2021 • 5 minutes to read

This article describes the steps to enable logging of the `Netlogon` service in Windows to monitor or troubleshoot authentication, DC locator, account lockout, or other domain communication-related issues.

Applies to: Windows 10 - all editions, Windows Server 2016, Windows Server 2019, Windows Server 2012 R2
Original KB number: 109626

More information

> **Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, click the following article number to view the article in the Microsoft Knowledge Base:
>
> 322756 How to back up and restore the registry in Windows

The version of Netlogon.dll that has tracing included is installed by default on all currently supported versions of Windows. To enable debug logging, set the debug flag that you want by using Nltest.exe, the registry, or Group Policy. To do it, follow these steps:

For Windows Server 2019, Windows Server 2016, Windows Server 2012 R2

> **Note**
>
> These steps also apply to Windows 10.

To enable `Netlogon` logging:

1. Open a Command Prompt window (administrative Command Prompt window for Windows Server 2012 R2 and later versions).
2. Type the following command, and then press Enter:

   Console

   ```
   Nltest /DBFlag:2080FFFF
   ```

3. It's typically unnecessary to stop and restart the `Netlogon` service for Windows Server 2012 R2 or later to enable `Netlogon` logging. Netlogon-related activity is logged to %windir%\debug\netlogon.log. Verify new writes to this log to determine whether a restart of the `Netlogon` service is necessary. If you have to restart the service, open a Command Prompt window (administrative Command Prompt window for Windows 10, and Windows Server 2012 R2 and later versions). Then run the following commands:

   Console

   ```
   net stop netlogon
   net start netlogon
   ```

   Note

   - In some circumstances, you may have to perform an authentication against the system in order to obtain a new entry in the log to verify that logging is enabled.
   - Using the computer name may cause no new test authentication entry to be logged.

To disable `Netlogon` logging, follow these steps:

1. Open a Command Prompt window (administrative Command Prompt window for Windows Server 2012 R2 and higher).
2. Type the following command, and then press Enter:

   Console

   ```
   Nltest /DBFlag:0x0
   ```

3. It's typically unnecessary to stop and restart the `Netlogon` service for Windows Server 2012 R2 or later versions to disable `Netlogon` logging. Netlogon-related activity is logged to %windir%\debug\netlogon.log. Verify that no new information is being written to this log to determine whether a restart of the `Netlogon` service is necessary. If you have to restart the service, open a Command Prompt window (administrative Command Prompt window for Windows 10, and Windows Server 2012 R2 and later versions). Then run the following commands:

   Console

   ```
   net stop netlogon
   net start netlogon
   ```

Alternative methods to enable Netlogon logging

- In all versions of Windows, you can use the registry method that's provided in the Enable/Disable logging by using registry method section.
- On computers that are running Windows Server 2012 R2 and later versions of the operating system, you can also use the following policy setting to enable verbose `Netlogon` logging (value is set in bytes):

  \Computer Configuration\Administrative Templates\System\Net Logon\Specify log file debug output level

> ⓘ **Note**
>
> - A value of decimal 545325055 is equivalent to 0x2080FFFF (which enables verbose `Netlogon` logging). This Group Policy setting is specified in bytes.
> - The Group Policy method can be used to enable `Netlogon` logging on a larger number of systems more efficiently. We don't recommend that you enable `Netlogon` logging in policies that apply to all systems, such as the Default Domain Policy. Instead, consider narrowing the scope to systems that may be causing problems by using one of the following methods:
>   - Create a new policy by using this Group Policy setting, and then provide the Read and Apply Group Policy rights to a group that contains only the required computer accounts.
>   - Move computer objects into a different OU, and then apply the policy settings at that OU level.

Enable/Disable logging by using registry method

To enable logging, you may have to obtain a checked build of Netlogon.dll.

1. Start Registry Editor.
2. If it exists, delete the Reg_SZ value of the following registry entry, create a REG_DWORD value with the same name, and then add the 2080FFFF hexadecimal value:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DBFlag`
3. It's typically unnecessary to stop and restart the `Netlogon` service for Windows Server 2012 R2 and later versions to enable `Netlogon` logging. Netlogon-related activity is logged to %windir%\debug\netlogon.log. Verify the new writes to this log to determine whether a restart of the `Netlogon` service is necessary. If you have to restart the service, open a Command Prompt window (administrative Command Prompt window for Windows Server 2012 R2/Windows 10 and above). Then run the following commands:

   Console

   ```
   net stop netlogon
   net start netlogon
   ```

> **Note**
>
> - In some circumstances, you may have to do an authentication against the system to obtain a new entry in the log to verify that logging is enabled.
> - Using the computer name may cause no new test authentication entry to be logged.

To disable `Netlogon` logging, follow these steps:

1. In Registry Editor, change the data value to 0x0 in the following registry key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DBFlag`
2. Exit Registry Editor.

3. It's typically unnecessary to stop and restart the `Netlogon` service for Windows Server 2012 R2, Windows 10, or later versions to disable `Netlogon` logging. Netlogon-related activity is logged to %windir%\debug\netlogon.log. Verify that no new information is being written to this log to determine whether a restart of the `Netlogon` service is necessary. If you have to restart the service, open a Command Prompt window (administrative Command Prompt window for Windows Server 2012 R2/Windows 10 and later versions of the operating system). Then run the following commands:

   Console

   ```
   net stop netlogon
   net start netlogon
   ```

Set the maximum log file size for `Netlogon` logs:

- The **MaximumLogFileSize** registry entry can be used to specify the maximum size of the Netlogon.log file. By default, this registry entry doesn't exist, and the default maximum size of the Netlogon.log file is 20 MB. When the file reaches 20 MB, it's renamed to Netlogon.bak, and a new Netlogon.log file is created. This registry entry has the following parameters:
  - Path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`
  - Value Name: MaximumLogFileSize
  - Value Type: REG_DWORD
  - Value Data: <maximum log file size in bytes>

- Remember that the total disk space that's used by `Netlogon` logging is the size that's specified in the maximum log file size times two (2). It's required to accommodate space for the Netlogon.log and Netlogon.bak file. For example, a setting of 50 MB can require 100 MB of disk space, which provides 50 MB for Netlogon.log and 50 MB for Netlogon.bak.

- As mentioned earlier, on Windows Server 2012 R2 and later versions of the operating system, you can use the following policy setting to configure the log file size (value is set in bytes):

  \Computer Configuration\Administrative Templates\System\Net Logon\Maximum Log File Size

For more information, click the following article numbers to view the articles in the Microsoft Knowledge Base:
247811 How domain controllers are located in Windows

How permissions are handled when you copy and move files and folders

Article • 09/23/2021 • 3 minutes to read

This article describes how Windows Explorer handles file and folder permissions in different situations.

Applies to: Windows 10 - all editions, Windows Server 2012 R2
Original KB number: 310316

Summary

In Microsoft Windows 2000, in Windows Server 2003, and in Windows XP, you have the option of using either the FAT32 file system or the NTFS file system. When you use NTFS, you can grant permissions to your folders and files to control access to those objects. When you copy or move a file or folder on an NTFS volume, how Windows Explorer handles the permissions on the object varies, depending on whether the object is copied or moved within the same NTFS volume or to a different volume.

More information

By default, an object inherits permissions from its parent object, either at the time of creation or when it is copied or moved to its parent folder. The only exception to this rule occurs when you move an object to a different folder on the same volume. In this case, the original permissions are retained.

Additionally, note the following rules:

- The Everyone group is granted **Allow Full Control** permissions to the root of each NTFS drive.
- Deny permissions always take precedence over **Allow** permissions.
- Explicit permissions take precedence over inherited permissions.
- If NTFS permissions conflict, for example, if group and user permissions are contradictory, the most liberal permissions take precedence.
- Permissions are cumulative.

- To preserve permissions when files and folders are copied or moved, use the Xcopy.exe utility with the `/O` or the `/X`switch.

  The object's original permissions will be added to inheritable permissions in the new location.

- To add an object's original permissions to inheritable permissions when you copy or move an object, use the Xcopy.exe utility with the `-O` and `-X` switches.

- To preserve existing permissions without adding inheritable permissions from the parent folder, use the Robocopy.exe utility, which is available in the Windows 2000 Resource Kit.

You can modify how Windows Explorer handles permissions when objects are copied or moved to another NTFS volume. When you copy or move an object to another volume, the object inherits the permissions of its new folder. However, if you want to modify this behavior to preserve the original permissions, modify the registry as follows.

> **ⓘ Important**
>
> This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see **How to back up and restore the registry in Windows**.

1. Click **Start**, click **Run**, type *regedit* in the **Open** box, and then press ENTER.
2. Locate and then click the registry key:
   `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer`.
3. On the **Edit** menu, click **Add Value**, and then add the following registry value:
   - Value name: ForceCopyAclwithFile
   - Data type: DWORD
   - Value data: 1
4. Exit Registry Editor.

You can modify how Windows Explorer handles permissions when objects are moved in the same NTFS volume. As mentioned, when an object is moved within the same volume, the object preserves its permissions by default. However, if you want to modify

this behavior so that the object inherits the permissions from the parent folder, modify the registry as follows:

1. Click **Start**, click **Run**, type *regedit*, and then press ENTER.
2. Locate and then click the registry subkey: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer`.
3. On the **Edit** menu, click **Add Value**, and then add the following registry value:
    - Value name: MoveSecurityAttributes
    - Data type: DWORD
    - Value data: 0
4. Exit Registry Editor.
5. Make sure that the user account that is used to move the object has the **Change Permissions** permission set. If the permission is not set, grant the **Change Permissions** permission to the user account.

> ⓘ **Note**
>
> The **MoveSecurityAttributes** registry value only applies to Windows XP and to Windows Server 2003. The value does not affect Windows 2000.

Unable to boot if more than one EFI system partition is present

Article • 09/23/2021 • 2 minutes to read

This article helps work around an issue where you can't boot Windows that was on the primary hard disk and may only have the option to boot to the new installation of Windows on the second hard disk.

Applies to: Windows Server 2012 R2, Windows 10 – all editions
Original KB number: 2879602

Symptoms

Consider the following scenario:

- You have a PC that is running Windows and is booting in uEFI mode.
- You add a second hard disk to the PC and start a second installation of Windows using uEFI bootable media. A new EFI System Partition (ESP) is created on the second disk in addition to the existing ESP on the primary hard disk.

In this scenario, after completing setup, you may no longer be able to boot to Windows that was on the primary hard disk and may only have the option to boot to the new installation of Windows on the second hard disk.

Cause

With the uEFI boot process, there's a reliance on the uEFI firmware boot entries presented during boot. The Windows installation process will append the latest installation to the list of available operating system and then set the most recent installation as the default boot option. This menu isn't typically exposed when booting the PC.

Because of variances in different versions of uEFI firmware, Windows doesn't make provisions for previously installed operating systems and as a result, doesn't currently support booting to multiple ESPs in the way described in the Symptoms section.

Workaround

The only Microsoft supported workaround for booting multiple installations of Windows in a uEFI environment is to use a dual boot configuration. This will make use of a single ESP and one MSR while still allowing the user to choose to boot to an installation on disk 1 or disk 2.

Note: The EFI firmware will use the last Windows installation (using setup.exe) as the primary boot OS.

More information

You may also encounter this issue if a second hard drive is added that has a pre-existing EFI partition and bootable OS on it as well. Because of differences in hardware and firmware boot options, it's unknown which Windows OS will be set as the primary boot disk.

Clear TPM fails with error code: 0x80290300

Article • 12/06/2021 • 2 minutes to read

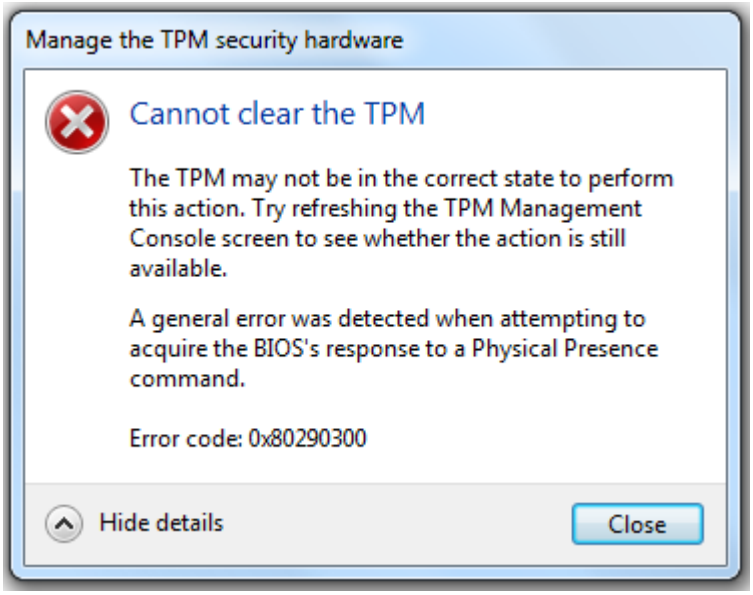
This article helps fix the error code 0x80290300 that occurs when you try to clear the TPM information.

Applies to: Window 10 – all editions
Original KB number: 2561178

Symptoms

On certain laptops or notebooks, when you attempt to clear TPM information you may receive the following error:

> 0x80290300: A general error was detected when attempting to acquire the BIOS's response to a Physical Presence command.



Cause

This issue is likely to happen when you have options like "RESET of TPM from OS" or "OS Management of TPM" disabled in the BIOS.

Resolution

Enable "RESET of TPM from OS" and "OS Management of TPM" option under System BIOS -> Security -> TPM Embedded Security page. Once done, this should help clear the TPM from operating system.

More information

To help protect against malware taking control of your computer's Trusted Platform Module (TPM) security hardware, computer manufacturers require users to establish "physical presence" before performing administrative tasks on the TPM, such as:

- Clearing an existing Owner from the TPM. (TPM_ForceClear Command)
- Temporarily deactivating a TPM. (TPM_SetTempDeactivated Command)
- Temporarily disabling a TPM. (TPM_PhysicalDisable Command)

Physical presence implies a level of control and authorization to perform basic administrative tasks and to bootstrap management and access control mechanisms.

Clearing the TPM cancels the TPM ownership and resets it to factory defaults. This should be done when a TPM-equipped client computer is recycled, or when the TPM owner has lost the TPM owner password.

You can clear the TPM or perform a limited number of TPM management tasks without entering the TPM owner password by just being present at the computer (Runs TPM_ForceClear Command). A physical presence isn't required to clear the TPM, if you have the TPM owner password (Runs TPM_OwnerClear command).

CAUTION: Clearing the TPM resets it to factory defaults. You'll lose all created keys and any data protected only by those keys.

For more information about TPM and how to manage TPM in Windows, see the TechNet Article Windows Trusted Platform Module Management Step-by-Step Guide.

For information about how to modify the BIOS, contact the BIOS manufacturer.

A Trusted Platform Module (TPM) isn't recognized on some Windows 7 devices

Article • 09/23/2021 • 2 minutes to read

This article solves the issue that a TPM isn't recognized as a compatible device on some Windows 7 devices.

Applies to: Windows 10 - all editions
Original KB number: 2895212

Symptoms

On some Windows 7 devices, a TPM isn't recognized as a compatible device. And it can't be used for certain applications, such as BitLocker Drive Encryption and Virtual Smart Card. Additionally, if you check the status of the TPM by using Windows TPM Management Console, you receive a **Compatible TPM cannot be found** message.

Also, you may experience the same behavior on some Windows-based devices when you do an in-place upgrade from Windows XP or Windows Vista to Windows 7.

Cause

This issue occurs because the TPM is using the OEM driver and not the Windows built-in Trusted Platform Module driver.

> **Note**
>
> When you open Device Manager on some devices, the TPM is listed under **System Devices** and not under **Security Devices**.

Resolution

To resolve this issue, open Device Manager on the device on which you're experiencing the issue, and then uninstall the Trusted Platform Module driver.

If you do a hardware scan, the TPM will be detected as a security device and will use the Microsoft driver. Additionally, the TPM will now be listed under **Security Devices** as Trusted Platform Module 1.2.

More information

For more information, see:

- Trusted Platform Module Technology Overview
- Initialize and Configure Ownership of the TPM

(0x6 ERROR_INVALID_HANDLE) error when a multithreaded application accesses a smart card

Article • 09/23/2021 • 2 minutes to read

This article describes how to troubleshoot and fix the "0x6 ERROR_INVALID_HANDLE" error that occurs when a multithreaded application accesses a smart card.

Applies to: Windows 10

Symptoms

Consider the following scenario:

- You have a smart card-enabled multithreaded application.
- The application is accessing a smart card that is based on the Microsoft Base Smart Card Cryptographic Service Provider (basecsp.dll/scksp.dll).
- The application runs for a while.

In this scenario, you receive a **0x6 ERROR_INVALID_HANDLE** error.

This problem occurs if a call is made to any Crypto API that uses the transaction manager, such as `CryptGetKeyParam()` and `CryptGetUserKey()`, to precede another call that releases the context.

The **ERROR_INVALID_HANDLE** error does not appear immediately. Depending on the load, it takes time for threads to encounter the synchronization problem.

Cause

This problem occurs because BaseCSP is not designed for high-load scenarios. Therefore, BaseCSP smart cards are neither thread-safe nor supported in high-load scenarios.

More information

BaseCSP can achieve thread safety only in typical usage scenarios, such as single user, smart card logon, email encryption or decryption, and code signing.

In typical usage scenarios, BaseCSP should be thread-safe per context. In high-load scenarios, BaseCSP smart cards encounter transaction manager synchronization problems.

Workaround

To work around this problem, use one of the following methods.

Method 1

Develop a vendor CSP or KSP provider, and implement a transaction manager in it. In this manner, the smart card subsystem will not use a transaction manager that is implemented in BaseCSP.

Method 2

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

A shorter transaction time-out can reduce the frequency of the problem. To achieve this, start **regedit**, and change the **TransactionTimeoutMilliseconds** value under the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\<provider_name>` subkey.

> **Note**
>
> In this subkey, <provider_name> is the BaseCSP or ksp, depending on the provider.

For detailed registry description, see Base CSP and Smart Card KSP registry keys.

For example, reducing **TransactionTimeoutMilliseconds** from its default value 1500 ms to 100 ms could reduce the frequency of the problem.

> **Important**
>
> This change is only a recommendation that's based on limited test results. There is no guarantee that reducing the **TransactionTimeoutMilliseconds** value will help to

control this problem. Additionally, changing the default value of **TransactionTimeoutMilliseconds** might cause some other problems to affect BaseCSP cards. Make sure that you thoroughly test your card for the relevant application and load before you deploy this change.

References

Base CSP and Smart Card KSP registry keys

Smart Card Minidrivers

winscard.h header

CryptGetKeyParam function (wincrypt.h)

CryptGetUserKey function (wincrypt.h)

Can't authenticate because of an incorrect PIV smart card driver update

Article • 12/06/2021 • 3 minutes to read

This article describes how to resolve a problem where users can't sign in to Windows until the incorrect driver is removed.

Applies to: Windows 10, version 2004, Windows 10, version 1909, Windows 10, version 1903
Original KB number: 4563240

Summary

If you use a Personal Identity Verification (PIV) smart card or any multifunction device that uses PIV smart cards that rely on the Windows Inbox Smart Card Minidriver, you may have received an incorrect driver update. When you try to use a smart card to authenticate to Windows, you might receive error messages such as "This smart card cannot be used" or "The operation requires a different smart card."

The incorrect update contains the "FEITIAN - SmartCard - 1.0.0.3" provider app that installs the Feitian xPass Smart Card driver. This is a legitimate, signed update that was published by a verified partner. However, it was inadvertently targeted to a broader set of devices than it was originally intended for.

The driver has been pulled from the Windows Update publishing system. To mitigate any adverse effects, any user who received the update has to manually roll back to the Windows inbox driver. For more information, see the "Resolution" section.

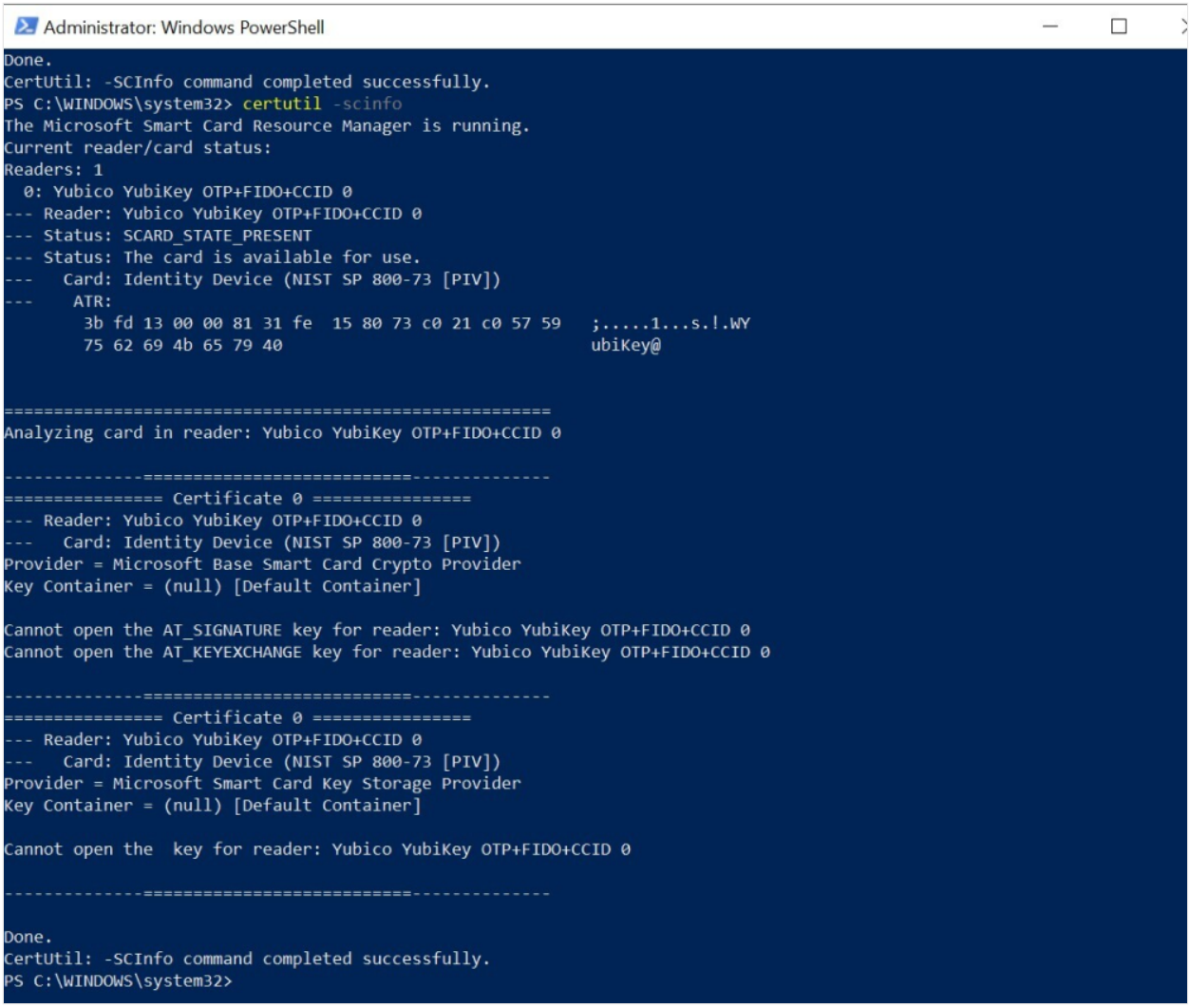
Symptoms

You observe one or more of the following symptoms:

- You try to sign in to Windows by using a PIV smart card or a device (such as a YubiKey) that supports PIV smart cards and relies on the Windows Inbox Smart Card Minidriver. However, you can't sign in.
- You try to sign in to Windows by using a non-Feitian-branded PIV smart card device. However, you can't sign in. If the device supports Fast Identity Online (FIDO) capabilities, such as U2F or FIDO2, those capabilities continue to work.
- The invalid xPass Smart Card driver doesn't correctly interface with other non-Feitian devices that rely on the inbox driver. This generates error messages such as

"This smart card cannot be used."

The following example shows the results of the **certutil -scinfo** command that runs on an affected computer. The certificates were generated as part of a Microsoft AD CS enrollment. However, they're no longer able to interface with the YubiKey PIV device after the xPass Smart Card driver is installed.



Cause

The Feitian xPass Smart Card driver version 1.0.0.3 specifies SCFILTER\CID_2777BE07-6993-4513-BD80-C184FCB0AB2D as a compatible identifier in the .inf file of its driver package. However, the Windows inbox smart card minidriver for PIV smart cards (Identity Device (NIST SP 800-73 [PIV])) uses the same compatible identifier. If you connect a non-Feitian device that uses the inbox driver to your computer, Windows recognizes the Feitian driver as compatible. Windows downloads, installs, and loads the Feitian driver.

For more information about how Windows selects drivers for a device, see Overview of the Driver Selection Process and How Windows selects a driver for a device.

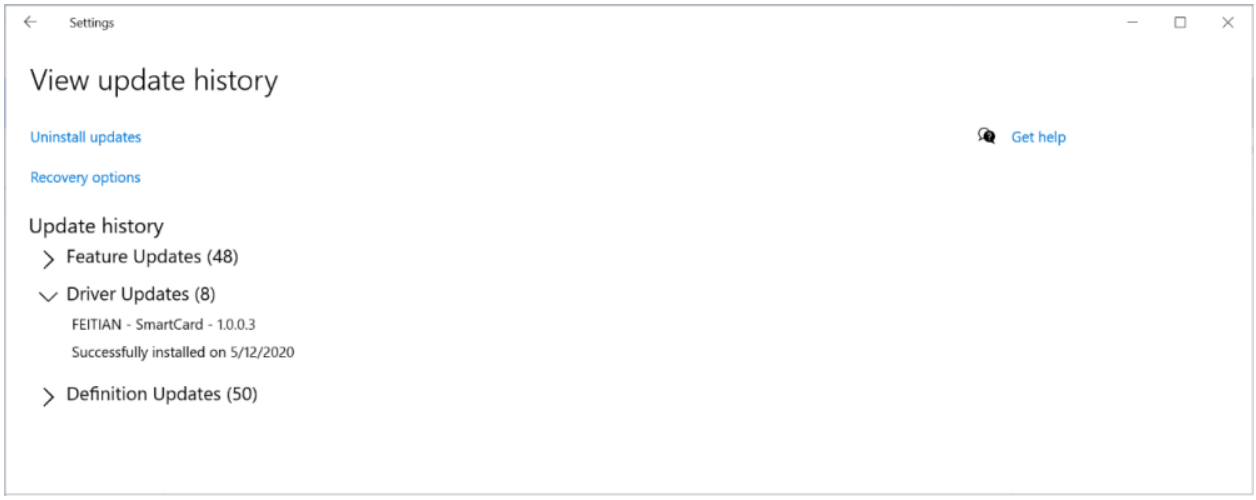
Resolution

If the Feitian xPass Smart Card driver has been installed on your computer, you have to remove it to revert to the inbox Identity Device (NIST SP 800-73 [PIV]) driver. After you remove the xPass Smart Card driver, Windows automatically loads the inbox driver for the device.

To do this, you can manually delete the driver, or create and run a script to delete it.

Determine whether your computer is affected

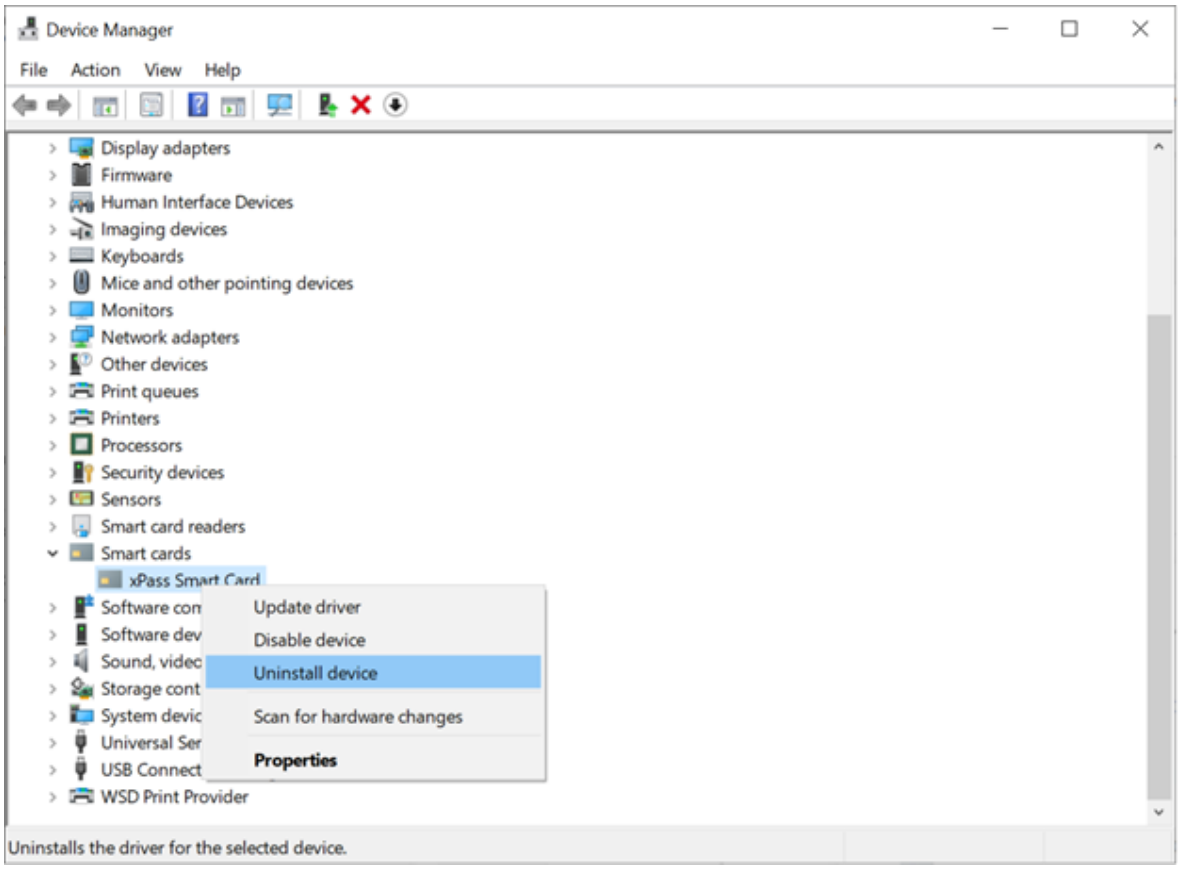
In Settings, select **Updates & Security** > **View update history**. You should be able to identify the driver update in the list.



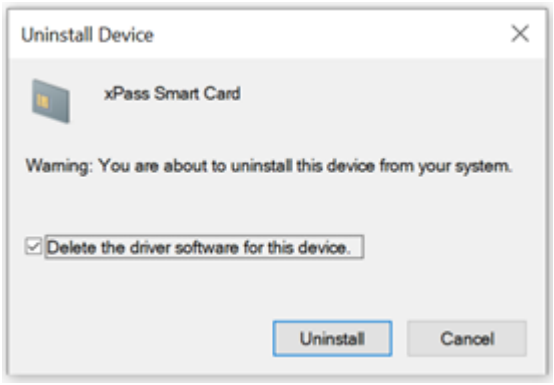
Manually delete the driver

To manually remove the driver, follow these steps:

1. Connect the smart card device to the computer.
2. Start Device Manager. You can start Device Manager from Control Panel, or by pressing **Windows** + **R**, and then entering **devmgmt.msc**.
3. Select **Smart cards**, right-click **xPass Smart Card**, and then select **Uninstall device**.



4. When you're prompted, select **Delete the driver software for this device**, and then select **Uninstall**.



Create a script to delete the driver

To automate the driver removal, create a script that can run in a batch file. The script identifies the driver .inf file name and uses PnPUtil.exe to delete the driver. The script can delete the driver even if a smart card or smart card device isn't connected to the computer. To create and use such a script, follow these steps:

1. Create a batch file that contains the following command sequence:

```
Console

@echo off
```

```
for /r %windir%\System32\DriverStore\FileRepository %%i in
(*eps_piv_csp11.inf*) do (@echo %%i
pnputil /delete-driver %%i /uninstall /force)

pause
```

2. On the affected computer, run the batch file in an administrative Command Prompt window.

More information

If you've followed the steps in the "Resolution" section but you need additional help, go to the Microsoft Support website.

Code 31 in Device Manager when Microsoft Usbccid Smartcard Reader is in a problem state

Article • 11/22/2021 • 2 minutes to read

Applies to: Windows 10

Symptoms

After a restart, Microsoft Usbccid Smartcard Reader is in a problem state with a yellow bang and this error is displayed in the device status:

> This device is not working properly because Windows cannot load the drivers required for this device. (Code 31)
> {Operation Failed}
> The requested operation was unsuccessful.

Cause

During initialization, the smartcard driver attempts to create an instance of smart card class extension. The attempt failed and the driver isn't loaded.

Resolution

To ensure a successful driver initialization, add the **RetryDeviceInitialize** registry key and restart the computer.

> **Note**
>
> The registry key is available for Windows 10, version 1903 (19H1) and later versions.

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\Readers`

Name: RetryDeviceInitialize
Type: DWORD (32-bit)
Data: 1

Event ID 14, 17 log for TPM command failure or non-recoverable error

Article • 09/23/2021 • 2 minutes to read

This article describes an issue in which the TPM device driver is recorded in the system log when it experiences an unrecoverable error.

Applies to: Windows 10 – all editions
Original KB number: 4562894

Symptoms

On a TPM device, you experience issues with BitLocker, logging to applications using Modern Authentication or Next Generation Credentials. These messages are logged in the event logs:

- The Trusted Platform Module (TPM) hardware failed to execute a TPM command.
- The device driver for the Trusted Platform Module (TPM) encountered a non-recoverable error in the TPM hardware, which prevents TPM services (such as data encryption) from being used.

See the following log examples for detailed information:

Event ID 14

> Log Name: System
> Source: TPM
> Date:
> Event ID: 14
> Task Category: None
> Level: Error
> Keywords:
> User: SYSTEM
> Computer: `WIN10PC.CONTOSO.COM`
> Description:
> The device driver for the Trusted Platform Module (TPM) encountered a non-recoverable error in the TPM hardware, which prevents TPM services (such as data encryption) from being used. For further help, please contact the computer manufacturer.

Event Xml:
<Event xmlns="`http://schemas.microsoft.com/win/2004/08/events/event`">
<System>
<Provider Name="TPM">
<EventID>14</EventID>
<Version>0</Version>
<Level>2</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords>
<EventRecordID>55474</EventRecordID>
<Correlation />
<Execution ProcessID="4" ThreadID="284" />
<Channel>System
<Computer>WIN10PC.CONTOSO.COM</Computer>
<Security UserID="S-1-5-18" />
</System>
<EventData>
<Data Name="locationCode">0x2c000230</Data>
<Data Name="Data">255</Data>
</EventData>
</Event>

Event ID 17

Log Name: System
Source: TPM
Date:
Event ID: 17
Task Category: None
Level: Information
Keywords:
User: SYSTEM
Computer: `WIN10PC.CONTOSO.COM`
Description:
The Trusted Platform Module (TPM) hardware failed to execute a TPM command.
Event Xml:
<Event xmlns="`http://schemas.microsoft.com/win/2004/08/events/event`">
<System>
<Provider Name="TPM">

<EventID>17</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords>
<EventRecordID>55475</EventRecordID>
<Correlation />
<Execution ProcessID="4" ThreadID="284" />
<Channel>System</Channel>
<Computer>WIN10PC.CONTOSO.COM</Computer>
<Security UserID="S-1-5-18" />
</System>
<EventData>
<Data Name="locationCode">0x1e000354</Data>
<Data Name="TpmCommandOrdinal">378</Data>
<Data Name="TpmResponseCode">3221225860</Data>
</EventData>
</Event>

Cause

This problem occurs because of an issue with the TPM device. It prevents Windows from communicating and using the TPM device for the functionalities that reply on TPM, such as:

- BitLocker
- Modern Authentication
- Next Generation Credentials

Workaround

Make sure the following updates are installed:

- Latest Servicing Stack Update (SSU) and monthly Cumulative Update (CU) in Windows
- Available update of the BIOS Firmware or TPM Device Firmware on manufacturer's support websites.

If the issue persists, contact the hardware vendor or the device manufacturer to diagnose your TPM device. For more information, see TPM Recommendations.

How to enable diagnostic logging for the Windows Security app

Article • 04/08/2022 • 2 minutes to read

This article describes how to enable diagnostic logging for the Windows Security app.

Applies to: Windows Server 2016, Windows 10, version 1809
Original KB number: 3155606

Summary

This article describes how to enable diagnostic logging for the Windows Security app in Windows 10.

More information

> **Important**
>
> Follow the steps in this section carefully. Serious problems might occur if you modify the registry incorrectly. Before you modify it, **back up the registry for restoration** in case problems occur.

To enable diagnostic logging for the Windows Security app, save the following content as a *.reg file, and then import the key:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\WscLogge
r]
"GUID"="{FFFAC41B-9B97-4DCA-98CE-611471DF0F85}"
"FileName"="%SystemRoot%\\System32\\LogFiles\\WMI\\WscTrace.etl"
"ClockType"=dword:00000002
"Start"=dword:00000001
"Status"=dword:00000000
"MaxFileSize"=dword:00000000
"FlushTimer"=dword:00000001
"LogFileMode"=dword:10000004

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\WscLogge
r\{1B0AC240-CBB8-4d55-8539-9230A44081A5}]
"Enabled"=dword:00000001
"EnableFlags"=dword:0000ffff
```

```
"EnableLevel"=dword:0000000f
"MatchAnyKeyword"=hex(b):ff,ff,ff,ff,00,00,00,00
```

For information about how to import registry data, see Import some or all of the registry.

The resulting log files are designed to be consumed by internal Microsoft teams, and they cannot be converted for use by using public tools.

After you create these keys, you have to restart the computer, and then data capture will start immediately. The data capture will occur across reboots and operating system upgrades.

To stop logging, change the Enabled value under the following key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\WscLogger{1B0AC240-CBB8-4d55-8539-9230A44081A5}

Windows Troubleshooters documentation

Article • 06/17/2021 • 2 minutes to read

The topic in this section provides information about Windows Troubleshooters.

Windows Troubleshooters topic

- Active and retired Windows 10 troubleshooters

Active and retired troubleshooters for Windows 10 and Windows 11

Article • 10/18/2022 • 5 minutes to read

This article provides a list of active and retired troubleshooters for Windows 10 and Windows 11, including a description of what the troubleshooter does, the problem that it addresses, and which devices it applies to. To learn more about troubleshooters, see keep your device running smoothly with recommended troubleshooting.

Applies to: Windows 10, Windows 11

Access work or school troubleshooter for restoring access to M365 desktop applications

Text displayed in Settings:
The troubleshooter checks if the Microsoft.AAD.BrokerPlugin package is missing. If so, it installs the package.

Description

Some users are unable to sign-in to Microsoft 365 desktop applications. This includes: Teams, Outlook, OneDrive for Business, Excel, PowerPoint, and Word.

This troubleshooter runs automatically on devices to meet the following criteria:

- Runs Windows 10, 20H1
- Enterprise and Pro SKUs of Microsoft 365
- Missing the package Microsoft.AAD.BrokerPlugin.

Activation date	Retirement date	More information
8/24/2022		https://aka.ms/AAhs34y

Windows Update troubleshooter for repairing .NET framework components

Text displayed in Settings:
Automatically repair system files and settings to fix a problem on your device

Description

Some devices that installed the April 25, 2022, update KB5012643 for Windows 11, version 21H2, are unable to run .NET Framework applications. This troubleshooter repairs the device by restoring the needed .NET Framework components and re-establishes the ability to run .NET Framework applications.

This troubleshooter runs automatically on devices that meet the following criteria:

- Runs Windows 10, version 21H2 and Windows 11, version 21H2
- This issue has been detected

Activation date	Retirement date	More information
5/31/2022		https://go.microsoft.com/fwlink/?linkid=2196115&clcid=0x409

Windows Update troubleshooter for file or metadata corruption

Text displayed in Settings:
Automatically targets the device for an In-Place Upgrade due to recurring installation issues

Description

Some devices that are running Windows 10, version 1903 and later versions can't install monthly security updates because of file or metadata corruption within the servicing stack. This troubleshooter marks the device in preparation for an In-Place Upgrade.

This troubleshooter runs automatically on devices that meet the following criteria:

- Runs one of these operating systems: Windows 10, versions 1903, Windows 10, version 1909, Windows 10, version 2004 or Windows 10, version 20H2
- Runs a revision below the December 2020 Security Update (12B)
- Failed a Quality Update installation multiple times

Activation date	Retirement date	More information
4/19/2021		aka.ms/IPUTroubleshooter

Windows Update troubleshooter for repairing system files

Text displayed in Settings:
Automatically repair system files and settings to improve device security

Description

Some devices running Windows 10, version 1903 or 1909 are not scanning for updates. This troubleshooter resets the update scanning process, which prompts the device to start a new scan.

This troubleshooter runs automatically on devices running Windows 10, version 1903 or 1909 and that have reported the error to the sediment infrastructure.

Activation date	Retirement date	More information
4/15/2021	11/2/2021	https://aka.ms/AAbk72i

Files On-Demand troubleshooter

Text displayed in Settings:
You may have lost access to your Files On-Demand. This troubleshooter restores access or prevents the loss of access from happening in the near future. Important: Please reboot your device once the troubleshooter is finished.

Description

After updating to Windows 10, version 2004, some older devices or devices that have certain older apps installed that use legacy file system filter drivers might be unable to connect to OneDrive through the OneDrive app. Affected devices might not be able to download new Files On-Demand content or open previously synced or downloaded files. This troubleshooter mitigates the issue.

Devices that successfully ran the "Hardware and Devices" troubleshooter will be notified and asked to run this troubleshooter.

Activation date	Retirement date	More information
6/30/2020	9/30/2020	https://aka.ms/AA8vtwr

Hardware and Devices troubleshooter for OneDrive

Text displayed in Settings:
Automatically repair system files and settings to fix a problem on your device.

Description

After updating to Windows 10, version 2004, some older devices or devices that have certain older apps installed that use legacy file system filter drivers might be unable to connect to OneDrive through the OneDrive app. Affected devices might not be able to download new Files On-Demand content or open previously synced or downloaded files. This troubleshooter detects the presence of this issue.

This troubleshooter runs automatically on devices that meet the following criteria:

- Runs on Windows 10, version 2004
- Uses a Cloud files filter (OneDrive, iCloud, Workfolders)

Activation date	Retirement date	More information
6/30/2020	9/30/2020	https://aka.ms/AA8vtwr

Storage Spaces cleanup troubleshooter

Text displayed in Settings:
Automatically restore your previous settings and environment for Storage Spaces.

Description

Devices that use Parity Storage Spaces might not be able to use or access their Storage Spaces after you update to Windows 10, version 2004 (the May 2020 update) or Windows Server, version 2004. After KB4568831 has been applied to your device, this troubleshooter restores your previous Storage Spaces settings.

This troubleshooter runs automatically on devices that meet the following criteria:

Successfully ran the "Hardware and Devices" or "Storage Spaces" troubleshooter

Activation date	Retirement date	More information
7/30/2020	10/30/2020	https://aka.ms/AA8uojg

Storage space troubleshooter

Text displayed in Settings:
Data corruption was detected on your parity storage space. This troubleshooter takes actions to prevent further corruption. It also restores write access if the space was previously marked read-only. For more information and recommended actions, please see the link below.

Description

Devices that use Parity Storage Spaces might experience issues when they try to use or access their Storage Spaces after they update to Windows 10, version 2004 (the May 2020 Update) or Windows Server, version 2004. This troubleshooter mitigates the issue for some users and restores read and write access to your Parity Storage Spaces.

This troubleshooter runs automatically on devices that meet the following criteria.

Successfully ran the "Hardware and Devices" or "Storage Spaces" troubleshooter.

Activation date	Retirement date	More information
7/2/2020	10/2/2020	https://aka.ms/AA8uojg

Hardware and Devices troubleshooter for Parity Storage Spaces

Text displayed in Settings:
Automatically change system settings to fix a problem on your device.

Description

Devices that use Parity Storage Spaces might experience issues when they try to use or access their Storage Spaces after they are updated to Windows 10, version 2004 (the May 2020 Update) or Windows Server, version 2004. This troubleshooter helps prevent issues that affect the data on your Storage Spaces. After the troubleshooter runs, you will not be able to write to your Storage Spaces.

This troubleshooter runs two times on devices that meet the following criteria:

- Runs Windows 10, version 2004
- Uses Storage Spaces

The first time, the troubleshooter runs automatically. The second time, it notifies the user.

Activation date	Retirement date	More information
6/26/2020	9/26/2020	https://aka.ms/AA8uojg

Windows Update troubleshooter for Disk Cleanup

Text displayed in Settings:
Automatically change system settings to fix a problem on your device.

Description

Some devices might not start if Disk Cleanup runs after you install the Windows version 19041.21 update. This troubleshooter temporarily disables the feature to automatically run Disk Cleanup until devices install the Windows 10, version 19041.84 update.

This troubleshooter automatically runs two times. It runs the first time on all devices on Windows 10, version 19041.21. It then runs again after devices are upgraded to Windows 10, version 19041.84.

Activation date	Retirement date	More information
2/7/2020	-	https://aka.ms/AA7afc1

Introduction to TroubleShootingScript toolset (TSSv2)

Article • 03/31/2022 • 9 minutes to read

This article introduces the TroubleShootingScript Version 2 (TSSv2) toolset and provides answers to frequently asked questions.

Applies to: Supported versions of Windows Server and Windows Client

The TSSv2 toolset includes PowerShell-based tools and a framework for data collection and diagnostics. The toolset aims to resolve customer support cases efficiently and securely.

The toolset includes several PowerShell scripts and executable files, which are all signed by Microsoft. Depending on how the toolset is started, it uses one or more of those scripts and executables to collect the required logs.

You can download the toolset as a zip file (*TSSv2.zip*) from https://aka.ms/getTSS.

Prerequisites

Here are some prerequisites for the toolset to run properly:

- The TSSv2 toolset must be run by accounts with administrator privileges on the local system, and the end-user license agreement (EULA) must be accepted. Once the EULA is accepted, the TSSv2 toolset won't prompt the EULA again.
- The PowerShell script execution policy should be set to `RemoteSigned` for the process level by running the cmdlet `Set-ExecutionPolicy -scope Process -ExecutionPolicy RemoteSigned -Force` from an elevated PowerShell command prompt.

  > **Note**
  >
  > The process level changes only affect the current PowerShell session.

Logs collection and sharing process

The TSSv2 toolset supports collecting various logs for troubleshooting purposes. Microsoft support representatives may provide you with a certain TSSv2 cmdlet to

collect logs for a problem when working on a support case, such as:

- Event logs
- System configuration
- Configuration details for installed Microsoft services
- Performance monitor logs
- Windows Performance Recorder (WPR) traces
- Network traces
- Memory dumps
- Event Tracing for Windows (ETW) traces for various components

Here are the steps for the logs collection and sharing process:

> ⓘ **Note**
>
> The support representative will provide you with complete steps for downloading and data collection.

1. The support representative identifies the problem and provides a certain TSSv2 cmdlet to collect the proper logs.
2. Download the *TSSv2.zip* file and copy the file to the affected systems.
3. Extract the *TSSv2.zip* file to a local folder in the affected systems, and run the TSSv2 cmdlet(s) from an elevated PowerShell command prompt simultaneously.
4. When the issue is reproduced, stop the TSSv2 toolset by pressing any key. The logs are automatically zipped by TSSv2 afterwards.
5. Upload the logs to a Microsoft secure file transfer site, which the support representative provides.

The support representative will work on the logs for further troubleshooting and provide the next action plan.

Frequently asked questions (FAQs)

- Q1: Does the TSSv2 script change any setup or configuration of my system?

  A1: No, but a registry setting is required for enabling debug logging in some scenarios. The script sets the necessary key at the start of the data collection and reverts the key to the default value at the end of the data collection. It may also delete some caches (for example, the ARP cache or the name resolution cache) at the start of the data collection to observe the problem from the logs.

- Q2: Does the TSSv2 toolset put an additional load on the server?

A2: Some loggings (for example, network capturing, ETW tracing collection, and so on) that are started by the TSSv2 toolset might put a minor load on the system. The load is usually at ignorable levels. Contact your support representative when you see high CPU, memory, or disk usage after starting the TSSv2 toolset.

- Q3: Why can't we reproduce the issue when the TSSv2 toolset is running?

  A3: The TSSv2 toolset may delete all cached information at the start. It also starts the network capturing in a promiscuous mode, which changes the Network Interface Card (NIC) default behaviors. These changes might affect the issue, and the problems may disappear. Especially for particular timing issues, problems disappear because of the TSSv2 toolset's data collection. The data collection starts logging, which might affect the issue indirectly and change the situation.

- Q4: Why is the TSSv2 toolset not responding for a long time?

  A4: In some cases, the operating system's built-in commands run by the TSSv2 toolset might not respond or take a long time to complete. Contact your support representative if you experience this issue.

- Q5: Do I need to worry about disk space or anything else when I run the TSSv2 toolset for a long time?

  A5: All TSSv2 tracing is configured to run with ring buffers, so you can run the toolset for a long time if needed. The TSSv2 toolset also calculates disk space at the beginning of the data collection and may exit if there isn't sufficient disk space. If you see high disk usage after starting the TSSv2 toolset or have any other concerns about the disk usage of the toolset, contact your support representative.

- Q6: What should I do if I receive the following security warning when running the *.\TSSv2.ps1* script?

  ```
  Security Warning: Run only scripts that you trust. While scripts from the Internet can be useful, this script can potentially harm your computer. Do you want to run .\TSSv2.ps1? [D] Do not run [R] Run once [S] Suspend [?] Help (default is "D")
  ```

  A6: In rare situations, you may receive this security warning. You may unblock the script by using the cmdlet `PS C:\> Unblock-File -Path C:\TSSv2\TSSv2.ps1`. This script will unblock all other modules by using the cmdlet `Get-ChildItem -Recurse -Path C:\TSSv2\*.ps* | Unblock-File -Confirm:$false`.

End User License Agreement (EULA)

Select below to view MICROSOFT SOFTWARE LICENSE TERMS.

▼ **Microsoft Diagnostic Scripts and Utilities**

These license terms are an agreement between you and Microsoft Corporation (or one of its affiliates). IF YOU COMPLY WITH THESE LICENSE TERMS, YOU HAVE THE RIGHTS BELOW. BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS.

1. INSTALLATION AND USE RIGHTS. Subject to the terms and restrictions set forth in this license, Microsoft Corporation ("Microsoft") grants you ("Customer" or "you") a non-exclusive, non-assignable, fully paid-up license to use and reproduce the script or utility provided under this license (the "Software"), solely for Customer's internal business purposes, to help Microsoft troubleshoot issues with one or more Microsoft products, provided that such license to the Software does not include any rights to other Microsoft technologies (such as products or services). "Use" means to copy, install, execute, access, display, run or otherwise interact with the Software.

   You may not sublicense the Software or any use of it through distribution, network access, or otherwise. Microsoft reserves all other rights not expressly granted herein, whether by implication, estoppel or otherwise. You may not reverse engineer, decompile or disassemble the Software, or otherwise attempt to derive the source code for the Software, except and to the extent required by third party licensing terms governing use of certain open source components that may be included in the Software, or remove, minimize, block, or modify any notices of Microsoft or its suppliers in the Software. Neither you nor your representatives may use the Software provided hereunder: (i) in a way prohibited by law, regulation, governmental order or decree; (ii) to violate the rights of others; (iii) to try to gain unauthorized access to or disrupt any service, device, data, account or network; (iv) to distribute spam or malware; (v) in a way that could harm Microsoft's IT systems or impair anyone else's use of them; (vi) in any application or situation where use of the Software could lead to the death or serious bodily injury of any person, or to physical or environmental damage; or (vii) to assist, encourage or enable anyone to do any of the above.

2. DATA. Customer owns all rights to data that it may elect to share with Microsoft through using the Software. You can learn more about data collection and use in the help documentation and the privacy statement at https://aka.ms/privacy. Your use of the Software operates as your consent to these practices.

3. FEEDBACK. If you give feedback about the Software to Microsoft, you grant to Microsoft, without charge, the right to use, share and commercialize your feedback in any way and for any purpose. You will not provide any feedback that is subject

to a license that would require Microsoft to license its software or documentation to third parties due to Microsoft including your feedback in such software or documentation.

4. EXPORT RESTRICTIONS. Customer must comply with all domestic and international export laws and regulations that apply to the Software, which include restrictions on destinations, end users, and end use. For further information on export restrictions, visit https://aka.ms/exporting .

5. REPRESENTATIONS AND WARRANTIES. Customer will comply with all applicable laws under this agreement, including in the delivery and use of all data. Customer or a designee agreeing to these terms on behalf of an entity represents and warrants that it (i) has the full power and authority to enter into and perform its obligations under this agreement, (ii) has full power and authority to bind its affiliates or organization to the terms of this agreement, and (iii) will secure the permission of the other party prior to providing any source code in a manner that would subject the other party's intellectual property to any other license terms or require the other party to distribute source code to any of its technologies.

6. DISCLAIMER OF WARRANTY. THE SOFTWARE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL MICROSOFT OR ITS LICENSORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

7. LIMITATION ON AND EXCLUSION OF DAMAGES. IF YOU HAVE ANY BASIS FOR RECOVERING DAMAGES DESPITE THE PRECEDING DISCLAIMER OF WARRANTY, YOU CAN RECOVER FROM MICROSOFT AND ITS SUPPLIERS ONLY DIRECT DAMAGES UP TO U.S. .00. YOU CANNOT RECOVER ANY OTHER DAMAGES, INCLUDING CONSEQUENTIAL, LOST PROFITS, SPECIAL, INDIRECT, OR INCIDENTAL DAMAGES. This limitation applies to (i) anything related to the Software, services, content (including code) on third party Internet sites, or third party applications; and (ii) claims for breach of contract, warranty, guarantee, or condition; strict liability, negligence, or other tort; or any other claim; in each case to the extent permitted by applicable law. It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may

not apply to you because your state, province, or country may not allow the exclusion or limitation of incidental, consequential, or other damages.

8. BINDING ARBITRATION AND CLASS ACTION WAIVER. This section applies if you live in (or, if a business, your principal place of business is in) the United States. If you and Microsoft have a dispute, you and Microsoft agree to try for 60 days to resolve it informally. If you and Microsoft can't, you and Microsoft agree to binding individual arbitration before the American Arbitration Association under the Federal Arbitration Act ("FAA"), and not to sue in court in front of a judge or jury. Instead, a neutral arbitrator will decide. Class action lawsuits, class-wide arbitrations, private attorney-general actions, and any other proceeding where someone acts in a representative capacity are not allowed; nor is combining individual proceedings without the consent of all parties. The complete Arbitration Agreement contains more terms and is at https://aka.ms/arb-agreement-4. You and Microsoft agree to these terms.

9. LAW AND VENUE. If U.S. federal jurisdiction exists, you and Microsoft consent to exclusive jurisdiction and venue in the federal court in King County, Washington for all disputes heard in court (excluding arbitration). If not, you and Microsoft consent to exclusive jurisdiction and venue in the Superior Court of King County, Washington for all disputes heard in court (excluding arbitration).

10. ENTIRE AGREEMENT. This agreement, and any other terms Microsoft may provide for supplements, updates, or third-party applications, is the entire agreement for the software.