

Contents

Manage clients in Windows 10

Administrative Tools in Windows 10

Create mandatory user profiles

Connect to remote Azure Active Directory-joined PC

Join Windows 10 Mobile to Azure Active Directory

New policies for Windows 10

Group Policies that apply only to Windows 10 Enterprise and Windows 10 Education

Manage the Settings app with Group Policy

What version of Windows am I running

Reset a Windows 10 Mobile device

Transitioning to modern management

Windows 10 Mobile deployment and management guide

Windows libraries

Troubleshoot Windows 10 clients

Advanced troubleshooting for Windows networking

Advanced troubleshooting Wireless network connectivity

Advanced troubleshooting 802.1X authentication

Data collection for troubleshooting 802.1X authentication

Advanced troubleshooting for TCP/IP

Collect data using Network Monitor

Troubleshoot TCP/IP connectivity

Troubleshoot port exhaustion

Troubleshoot Remote Procedure Call (RPC) errors

Advanced troubleshooting for Windows startup

Advanced troubleshooting for Windows boot problems

Advanced troubleshooting for Windows-based computer freeze

Advanced troubleshooting for stop error or blue screen error

Advanced troubleshooting for stop error 7B or Inaccessible_Boot_Device

Mobile device management for solution providers

Change history for Client management

Client management

3/19/2019 • 2 minutes to read • [Edit Online](#)

Applies to

- Windows 10

Learn about the administrative tools, tasks and best practices for managing Windows 10 and Windows 10 Mobile clients across your enterprise.

TOPIC	DESCRIPTION
Administrative Tools in Windows 10	Links to documentation for tools for IT pros and advanced users in the Administrative Tools folder.
Create mandatory user profiles	Instructions for managing settings commonly defined in a mandatory profiles, including (but are not limited to): icons that appear on the desktop, desktop backgrounds, user preferences in Control Panel, printer selections, and more.
Connect to remote Azure Active Directory-joined PCs	Instructions for connecting to a remote PC joined to Azure Active Directory (Azure AD)
Join Windows 10 Mobile to Azure AD	Describes the considerations and options for using Windows 10 Mobile with Azure AD in your organization.
New policies for Windows 10	Listing of new group policy settings available in Windows 10
Group policies for enterprise and education editions	Listing of all group policy settings that apply specifically to Windows 10 Enterprise and Education editions
Manage the Settings app with Group Policy	Starting in Windows 10, version 1703, you can now manage the pages that are shown in the Settings app by using Group Policy.
Reset a Windows 10 Mobile device	Instructions for resetting a Windows 10 Mobile device using either <i>factory</i> or <i>'wipe and persist'</i> reset options
Transitioning to modern ITPro management	Describes modern Windows 10 ITPro management scenarios across traditional, hybrid and cloud-based enterprise needs
Windows 10 Mobile deployment and management guide	Considerations and instructions for deploying Windows 10 Mobile
Windows libraries	Considerations and instructions for managing Windows 10 libraries such as My Documents, My Pictures, and My Music.
Mobile device management for solution providers	Procedural and reference documentation for solution providers providing mobile device management (MDM) for Windows 10 devices.

TOPIC	DESCRIPTION
Change history for Client management	This topic lists new and updated topics in the Client management documentation for Windows 10 and Windows 10 Mobile.

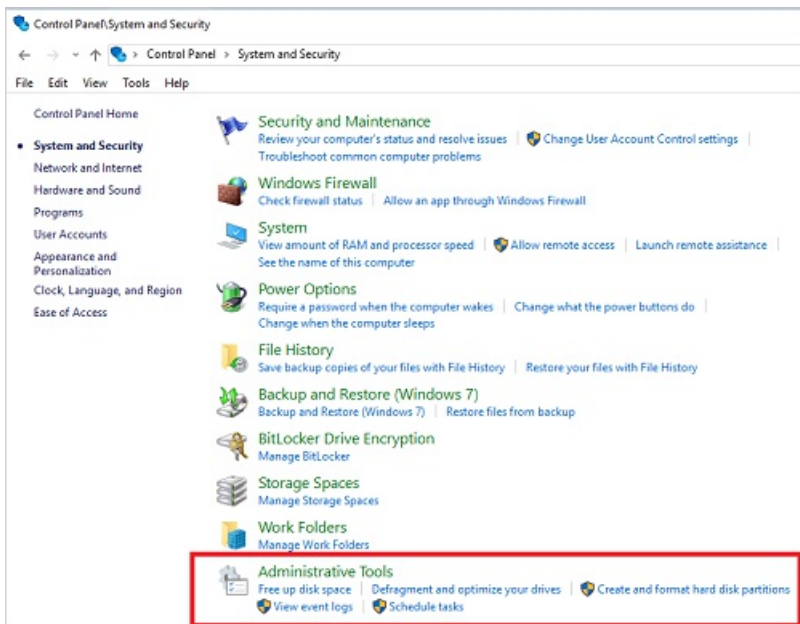
Administrative Tools in Windows 10

6/10/2019 • 2 minutes to read • [Edit Online](#)

Applies to

- Windows 10

Administrative Tools is a folder in Control Panel that contains tools for system administrators and advanced users.



The tools in the folder might vary depending on which edition of Windows you are using.

Name	Date modified
Component Services	4/6/2016 1:46 AM
Computer Management	4/6/2016 1:46 AM
Defragment and Optimize Drives	4/6/2016 1:46 AM
desktop.ini	4/6/2016 4:21 AM
Disk Cleanup	4/6/2016 1:50 AM
Event Viewer	4/6/2016 1:46 AM
iSCSI Initiator	4/6/2016 1:46 AM
Local Security Policy	4/6/2016 1:49 AM
ODBC Data Sources (32-bit)	4/6/2016 1:48 AM
ODBC Data Sources (64-bit)	4/6/2016 1:46 AM
Performance Monitor	4/6/2016 1:46 AM
Print Management	4/6/2016 1:49 AM
Resource Monitor	4/6/2016 1:46 AM
Services	4/6/2016 1:46 AM
System Configuration	4/6/2016 1:46 AM
System Information	4/6/2016 1:46 AM
Task Scheduler	4/6/2016 1:46 AM
Windows Firewall with Advanced Security	4/6/2016 1:46 AM
Windows Memory Diagnostic	4/6/2016 1:46 AM

These tools were included in previous versions of Windows and the associated documentation for each tool should help you use these tools in Windows 10. The following list links to documentation for each tool.

- [Component Services](#)

- [Computer Management](#)
- [Defragment and Optimize Drives](#)
- [Disk Cleanup](#)
- [Event Viewer](#)
- [iSCSI Initiator](#)
- [Local Security Policy](#)
- [ODBC Data Sources](#)
- [Performance Monitor](#)
- [Print Management](#)
- [Resource Monitor](#)
- [Services](#)
- [System Configuration](#)
- [System Information](#)
- [Task Scheduler](#)
- [Windows Firewall with Advanced Security](#)
- [Windows Memory Diagnostic](#)

TIP

If the content that is linked to a tool in the following list doesn't provide the information you need to use that tool, send us a comment by using the **Was this page helpful?** feature on this **Administrative Tools in Windows 10** page. Details about the information you want for a tool will help us plan future content.

Related topics

[Diagnostic Data Viewer](#)

Create mandatory user profiles

6/10/2019 • 6 minutes to read • [Edit Online](#)

Applies to

- Windows 10

A mandatory user profile is a roaming user profile that has been pre-configured by an administrator to specify settings for users. Settings commonly defined in a mandatory profile include (but are not limited to): icons that appear on the desktop, desktop backgrounds, user preferences in Control Panel, printer selections, and more. Configuration changes made during a user's session that are normally saved to a roaming user profile are not saved when a mandatory user profile is assigned.

Mandatory user profiles are useful when standardization is important, such as on a kiosk device or in educational settings. Only system administrators can make changes to mandatory user profiles.

When the server that stores the mandatory profile is unavailable, such as when the user is not connected to the corporate network, users with mandatory profiles can sign in with the locally cached copy of the mandatory profile, if one exists. Otherwise, the user will be signed in with a temporary profile.

User profiles become mandatory profiles when the administrator renames the NTuser.dat file (the registry hive) of each user's profile in the file system of the profile server from `NTuser.dat` to `NTuser.man`. The `.man` extension causes the user profile to be a read-only profile.

Profile extension for each Windows version

The name of the folder in which you store the mandatory profile must use the correct extension for the operating system it will be applied to. The following table lists the correct extension for each operating system version.

CLIENT OPERATING SYSTEM VERSION	SERVER OPERATING SYSTEM VERSION	PROFILE EXTENSION
Windows XP	Windows Server 2003 Windows Server 2003 R2	none
Windows Vista Windows 7	Windows Server 2008 Windows Server 2008 R2	v2
Windows 8	Windows Server 2012	v3
Windows 8.1	Windows Server 2012 R2	v4
Windows 10, versions 1507 and 1511	N/A	v5
Windows 10, versions 1607, 1703, 1709, 1803, and 1809	Windows Server 2016	v6

For more information, see [Deploy Roaming User Profiles, Appendix B](#) and [Roaming user profiles versioning in Windows 10 and Windows Server Technical Preview](#).

How to create a mandatory user profile

First, you create a default user profile with the customizations that you want, run Sysprep with CopyProfile set to **True** in the answer file, copy the customized default user profile to a network share, and then you rename the

profile to make it mandatory.

To create a default user profile

1. Sign in to a computer running Windows 10 as a member of the local Administrator group. Do not use a domain account.

NOTE

Use a lab or extra computer running a clean installation of Windows 10 to create a default user profile. Do not use a computer that is required for business (that is, a production computer). This process removes all domain accounts from the computer, including user profile folders.

2. Configure the computer settings that you want to include in the user profile. For example, you can configure settings for the desktop background, uninstall default apps, install line-of-business apps, and so on.

NOTE

Unlike previous versions of Windows, you cannot apply a Start and taskbar layout using a mandatory profile. For alternative methods for customizing the Start menu and taskbar, see [Related topics](#).

3. [Create an answer file \(Unattend.xml\)](#) that sets the [CopyProfile](#) parameter to **True**. The CopyProfile parameter causes Sysprep to copy the currently signed-on user's profile folder to the default user profile. You can use [Windows System Image Manager](#), which is part of the Windows Assessment and Deployment Kit (ADK) to create the Unattend.xml file.
4. Uninstall any application you do not need or want from the PC. For examples on how to uninstall Windows 10 Application see [Remove-AppxProvisionedPackage](#). For a list of uninstalleable applications, see [Understand the different apps included in Windows 10](#).

```
>[!NOTE]
```

```
>It is highly recommended to uninstall unwanted or unneeded apps as it will speed up user sign-in times.
```

3. At a command prompt, type the following command and press **ENTER**.

```
sysprep /oobe /reboot /generalize /unattend:unattend.xml
```

(Sysprep.exe is located at: C:\Windows\System32\sysprep. By default, Sysprep looks for unattend.xml in this same folder.)

TIP

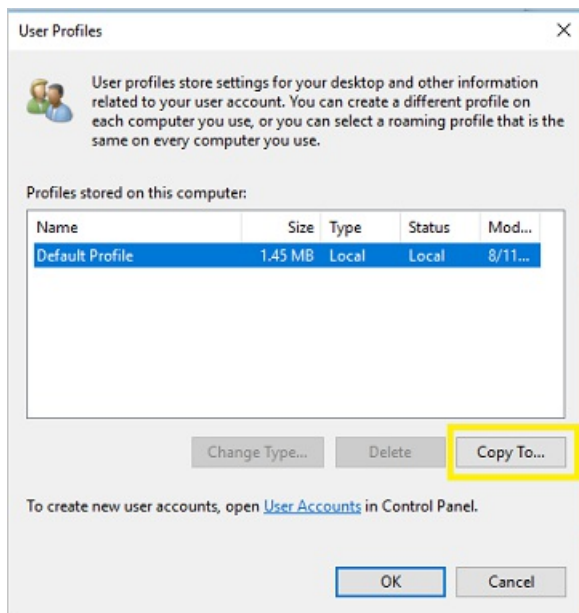
If you receive an error message that says "Sysprep was not able to validate your Windows installation", open %WINDIR%\System32\Sysprep\Panther\setupact.log and look for an entry like the following:

```
2016-08-11 14:19:20, Error                SYSPRP Package
Microsoft.BingTranslator_4.4.0.0_x86_8wekyb3d8bbwe was installed for a user, but not
provisioned for all users. This package will not function properly in the sysprep image.
```

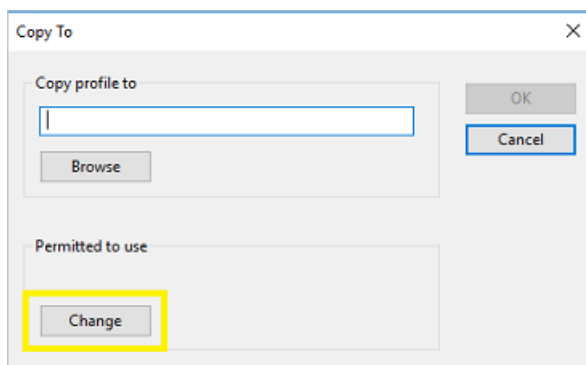
Use the [Remove-AppxProvisionedPackage](#) and [Remove-AppxPackage -AllUsers](#) cmdlet in Windows PowerShell to uninstall the app that is listed in the log.

4. The sysprep process reboots the PC and starts at the first-run experience screen. Complete the set up, and then sign in to the computer using an account that has local administrator privileges.

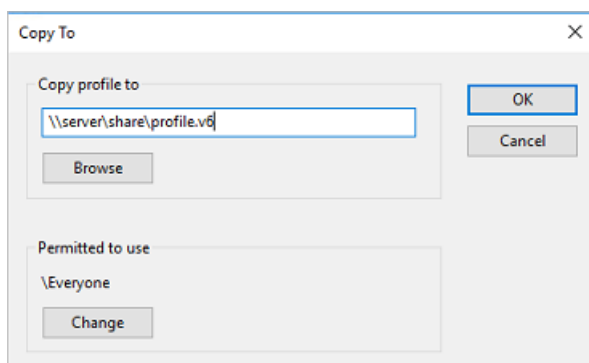
- Right-click Start, go to **Control Panel** (view by large or small icons) > **System** > **Advanced system settings**, and click **Settings** in the **User Profiles** section.
- In **User Profiles**, click **Default Profile**, and then click **Copy To**.



- In **Copy To**, under **Permitted to use**, click **Change**.



- In **Select User or Group**, in the **Enter the object name to select** field, type `everyone`, click **Check Names**, and then click **OK**.
- In **Copy To**, in the **Copy profile to** field, enter the path and folder name where you want to store the mandatory profile. The folder name must use the correct [extension](#) for the operating system version. For example, the folder name must end with ".v6" to identify it as a user profile folder for Windows 10, version 1607.
 - If the device is joined to the domain and you are signed in with an account that has permissions to write to a shared folder on the network, you can enter the shared folder path.
 - If the device is not joined to the domain, you can save the profile locally and then copy it to the shared folder location.



10. Click **OK** to copy the default user profile.

To make the user profile mandatory

3. In File Explorer, open the folder where you stored the copy of the profile.

NOTE

If the folder is not displayed, click **View > Options > Change folder and search options**. On the **View** tab, select **Show hidden files and folders**, clear **Hide protected operating system files**, click **Yes** to confirm that you want to show operating system files, and then click **OK** to save your changes.

4. Rename `Ntuser.dat` to `Ntuser.man`.

How to apply a mandatory user profile to users

In a domain, you modify properties for the user account to point to the mandatory profile in a shared folder residing on the server.

To apply a mandatory user profile to users

1. Open **Active Directory Users and Computers** (dsa.msc).
2. Navigate to the user account that you will assign the mandatory profile to.
3. Right-click the user name and open **Properties**.
4. On the **Profile** tab, in the **Profile path** field, enter the path to the shared folder without the extension. For example, if the folder name is `\\server\profile.v6`, you would enter `\\server\profile`.
5. Click **OK**.

It may take some time for this change to replicate to all domain controllers.

Apply policies to improve sign-in time

When a user is configured with a mandatory profile, Windows 10 starts as though it was the first sign-in each time the user signs in. To improve sign-in performance for users with mandatory user profiles, apply the Group Policy settings shown in the following table. (The table shows which operating system versions each policy setting can apply to.)

GROUP POLICY SETTING	WINDOWS 10	WINDOWS SERVER 2016	WINDOWS 8.1	WINDOWS SERVER 2012
Computer Configuration > Administrative Templates > System > Logon > Show first sign-in animation = Disabled	✓	✓	✓	✓

GROUP POLICY SETTING	WINDOWS 10	WINDOWS SERVER 2016	WINDOWS 8.1	WINDOWS SERVER 2012
Computer Configuration > Administrative Templates > Windows Components > Search > Allow Cortana = Disabled	✓	✓	✗	✗
Computer Configuration > Administrative Templates > Windows Components > Cloud Content > Turn off Microsoft consumer experience = Enabled	✓	✗	✗	✗

Related topics

- [Manage Windows 10 Start layout and taskbar options](#)
- [Lock down Windows 10 to specific apps](#)
- [Windows Spotlight on the lock screen](#)
- [Configure devices without MDM](#)

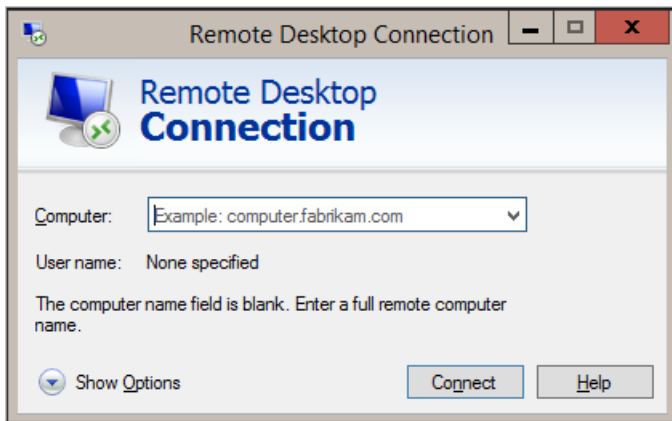
Connect to remote Azure Active Directory-joined PC

6/6/2019 • 2 minutes to read • [Edit Online](#)

Applies to

- Windows 10

From its release, Windows 10 has supported remote connections to PCs that are joined to Active Directory. Starting in Windows 10, version 1607, you can also connect to a remote PC that is [joined to Azure Active Directory \(Azure AD\)](#).

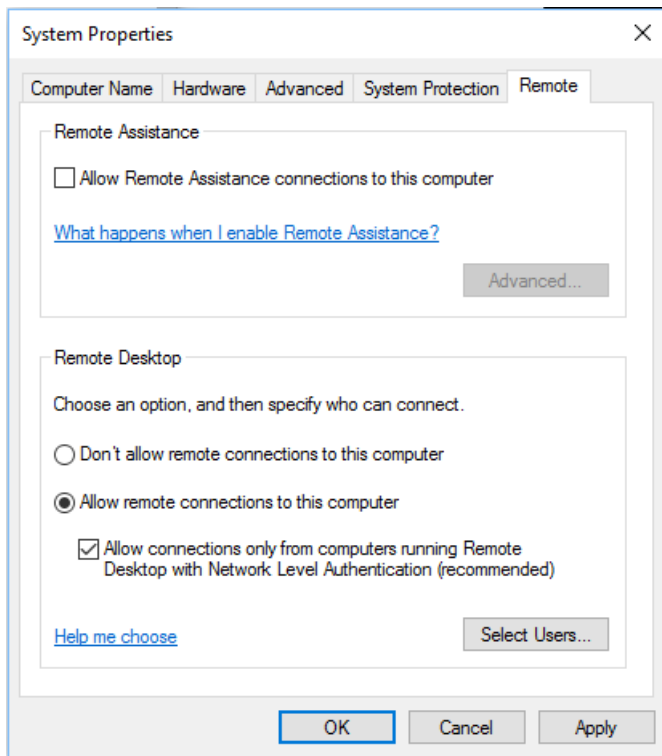


TIP

Starting in Windows 10, version 1809, you can [use biometrics to authenticate to a remote desktop session](#).

Set up

- Both PCs (local and remote) must be running Windows 10, version 1607 (or later). Remote connection to an Azure AD-joined PC that is running earlier versions of Windows 10 is not supported.
- Ensure [Remote Credential Guard](#), a new feature in Windows 10, version 1607, is turned off on the client PC that you are using to connect to the remote PC.
- On the PC that you want to connect to:
 1. Open system properties for the remote PC.
 2. Enable **Allow remote connections to this computer** and select **Allow connections only from computers running Remote Desktop with Network Level Authentication**.



3. If the user who joined the PC to Azure AD is the only one who is going to connect remotely, no additional configuration is needed. To allow additional users to connect to the PC, you must allow remote connections for the local **Authenticated Users** group. Click **Select Users**.

NOTE

You can specify individual Azure AD accounts for remote connections by having the user sign in to the remote device at least once and then running the following PowerShell cmdlet:

```
net localgroup "Remote Desktop Users" /add "AzureAD\the-UPN-attribute-of-your-user", where  
FirstnameLastname is the name of the user profile in C:\Users, which is created based on DisplayName  
attribute in Azure AD.
```

In Windows 10, version 1709, the user does not have to sign in to the remote device first.

In Windows 10, version 1709, you can add other Azure AD users to the **Administrators** group on a device in **Settings** and restrict remote credentials to **Administrators**. If there is a problem connecting remotely, make sure that both devices are joined to Azure AD and that TPM is functioning properly on both devices.

4. Enter **Authenticated Users**, then click **Check Names**. If the **Name Not Found** window opens, click **Locations** and select this PC.

TIP

When you connect to the remote PC, enter your account name in this format: `AzureAD UPN`. The local PC must either be domain-joined or Azure AD-joined. The local PC and remote PC must be in the same Azure AD tenant.

Supported configurations

In organizations that have integrated Active Directory and Azure AD, you can connect from a domain-joined PC to an Azure AD-joined PC using:

- Password
- Smartcards

- Windows Hello for Business, if the domain is managed by System Center Configuration Manager

In organizations that have integrated Active Directory and Azure AD, you can connect from an Azure AD-joined PC to an AD-joined PC when the Azure AD-joined PC is on the corporate network using:

- Password
- Smartcards
- Windows Hello for Business, if the organization has a mobile device management (MDM) subscription.

In organizations that have integrated Active Directory and Azure AD, you can connect from an Azure AD-joined PC to another Azure AD-joined PC using:

- Password
- Smartcards
- Windows Hello for Business, with or without an MDM subscription.

In organizations using only Azure AD, you can connect from an Azure AD-joined PC to another Azure AD-joined PC using:

- Password
- Windows Hello for Business, with or without an MDM subscription.

Related topics

[How to use Remote Desktop](#)

Join Windows 10 Mobile to Azure Active Directory

5/31/2019 • 10 minutes to read • [Edit Online](#)

Applies to

- Windows 10 Mobile

Devices running Windows 10 Mobile can join Azure Active Directory (Azure AD) when the device is configured during the out-of-box experience (OOBE). This article describes the considerations and options for using Windows 10 Mobile with Azure AD in your organization.

Why join Windows 10 Mobile to Azure AD

When a device running Windows 10 Mobile is joined to Azure AD, the device can exclusively use a credential owned by your organization, and you can ensure users sign in using the sign-in requirements of your organization. Joining a Windows 10 Mobile device to Azure AD provides many of the same benefits as joining desktop devices, such as:

- Single sign-on (SSO) in applications like Mail, Word, and OneDrive using resources backed by Azure AD.
- SSO in Microsoft Edge browser to Azure AD-connected web applications like Office 365 Portal, Visual Studio, and more than [2500 non-Microsoft apps](#).
- SSO to resources on-premises.
- Automatically enroll in your mobile device management (MDM) service.
- Enable enterprise roaming of settings. (Not currently supported but on roadmap)
- Use Microsoft Store for Business to target applications to users.

Are you upgrading current devices to Windows 10 Mobile?

Windows Phone 8.1 only supported the ability to connect the device to personal cloud services using a Microsoft account for authentication. This required creating Microsoft accounts to be used for work purposes. In Windows 10 Mobile, you have the ability to join devices directly to Azure AD without requiring a personal Microsoft account.

If you have existing Windows Phone 8.1 devices, the first thing to understand is whether the devices you have can be upgraded to Windows 10 Mobile. Microsoft will be releasing more information about upgrade availability soon. As more information becomes available, it will be posted at [How to get Windows 10 Mobile](#). Premier Enterprise customers that have a business need to postpone Windows 10 Mobile upgrade should contact their Technical Account Manager to understand what options may be available.

Before upgrading and joining devices to Azure AD, you will want to consider existing data usage. How users are using the existing devices and what data is stored locally will vary for every customer. Are text messages used for work purposes and need to be backed up and available after the upgrade? Are there photos stored locally or stored associated with an Microsoft account? Are there device and app settings that to be retained? Are there contacts stored in the SIM or associated with an Microsoft account? You will need to explore methods for capturing and storing the data that needs to be retained before you join the devices to Azure AD. Photos, music files, and documents stored locally on the device can be copied from the device using a USB connection to a PC.

To join upgraded mobile devices to Azure AD, [the devices must be reset](#) to start the out-of-box experience for device setup. Joining a device to Azure AD is not a change that can be done while maintaining existing user data.

This is similar to changing a device from personally owned to organizationally owned. When a user joins an organization's domain, the user is then required to log in as the domain user and start with a fresh user profile. A new user profile means there would not be any persisted settings, apps, or data from the previous personal profile.

If you want to avoid the device reset process, consider [adding work accounts](#) rather than joining the devices to Azure AD.

The difference between "Add work account" and "Azure AD Join"

Even though Azure AD Join on Windows 10 Mobile provides the best overall experience, there are two ways that you can use an added work account instead of joining the device to Azure AD due to organizational requirements.

- You can complete OOBЕ using the **Sign in later** option. This lets you start using Windows 10 Mobile with any connected Azure AD account or Microsoft account.
- You can add access to Azure AD-backed resources on the device without resetting the device.

However, neither of these methods provides SSO in the Microsoft Store or SSO to resources on-premises, and does not provide the ability to roam settings based on the Azure AD account using enterprise roaming. [Learn about enterprise state roaming in Azure AD.](#)

Using **Settings > Accounts > Your email and accounts > Add work or school account**, users can add their Azure AD account to the device. Alternatively, a work account can be added when the user signs in to an application like Mail, Word, etc. If you [enable auto-enrollment in your MDM settings](#), the device will automatically be enrolled in MDM.

An added work account provides the same SSO experience in browser apps like Office 365 (Office portal, Outlook on the web, Calendar, People, OneDrive), Azure AD profile and change password app, and Visual Studio. You get SSO to built-in applications like Mail, Calendar, People, OneDrive and files hosted on OneDrive without prompts for a password. In Office apps like Microsoft Word, Microsoft Excel, etc., you simply select the Azure AD account and you are able to open files without entering a password.

Preparing for Windows 10 Mobile

• Azure AD configuration

Currently, Azure AD Join only supports self-provisioning, meaning the credentials of the user of the device must be used during the initial setup of the device. If your mobile operator prepares devices on your behalf, this will impact your ability to join the device to Azure AD. Many IT administrators may start with a desire to set up devices for their employees, but the Azure AD Join experience is optimized for end-users, including the option for automatic MDM enrollment.

By default, Azure AD is set up to allow devices to join and to allow users to use their corporate credentials on organizational-owned devices or personal devices. The blog post [Azure AD Join on Windows 10 devices](#) has more information on where you can review your Azure AD settings. You can configure Azure AD to not allow anyone to join, to allow everyone in your organization to join, or you can select specific Azure AD groups which are allowed to join.

• Device setup

A device running Windows 10 Mobile can only join Azure AD during OOBЕ. New devices from mobile operators will be in this state when they are received. Windows Phone 8.1 devices that are [upgraded](#) to Windows 10 Mobile will need to be reset to get back to OOBЕ for device setup.

• Mobile device management

An MDM service is required for managing Azure AD-joined devices. You can use MDM to push settings to

devices, as well as application and certificates used by VPN, Wi-Fi, etc. Azure AD Premium or [Enterprise Mobility Suite \(EMS\)](#) licenses are required to set up your Azure AD-joined devices to automatically enroll in MDM. [Learn more about setting up your Azure AD tenant for MDM auto-enrollment.](#)

- **Windows Hello**

Creating a Windows Hello (PIN) is required on Windows 10 Mobile by default and cannot be disabled. You can control Windows Hello policies using controls in MDM, such as Intune. Because the device is joined using organizational credentials, the device must have a PIN to unlock the device. Biometrics such as fingerprint or iris can be used for authentication. Creating a Windows Hello requires the user to perform a multi-factor authentication since the PIN is a strong authentication credential. [Learn more about Windows Hello for Azure AD.](#)

- **Conditional access**

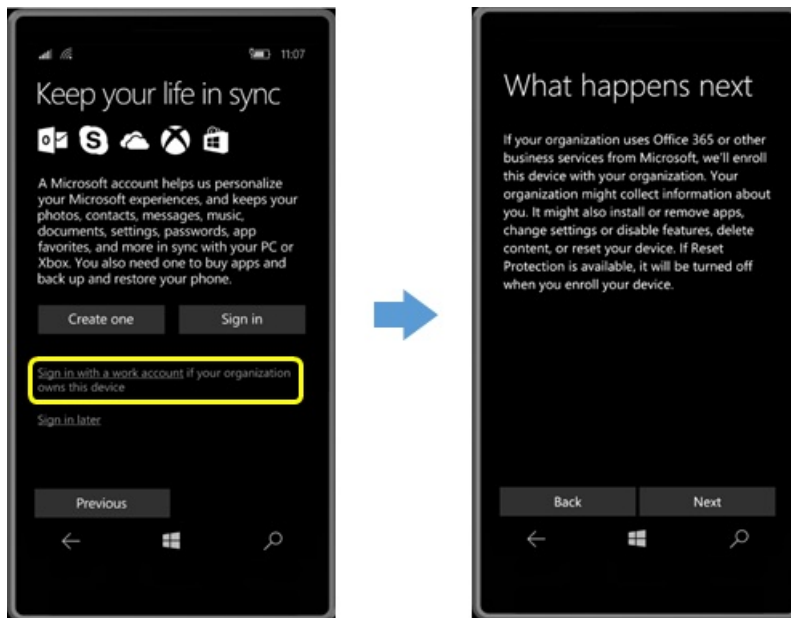
Conditional access policies are also applicable to Windows 10 Mobile. Multifactor authentication and device compliance policies can be applied to users or resources and require that the user or device satisfies these requirements before access to resources is allowed. Policies like **Domain Join** which support traditional domain joining only apply to desktop PC. Policies dependent on IP range will be tough to enforce on a phone as the IP address of the operator is used unless the user has connected to corporate Wi-Fi or a VPN.

- **Known issues**

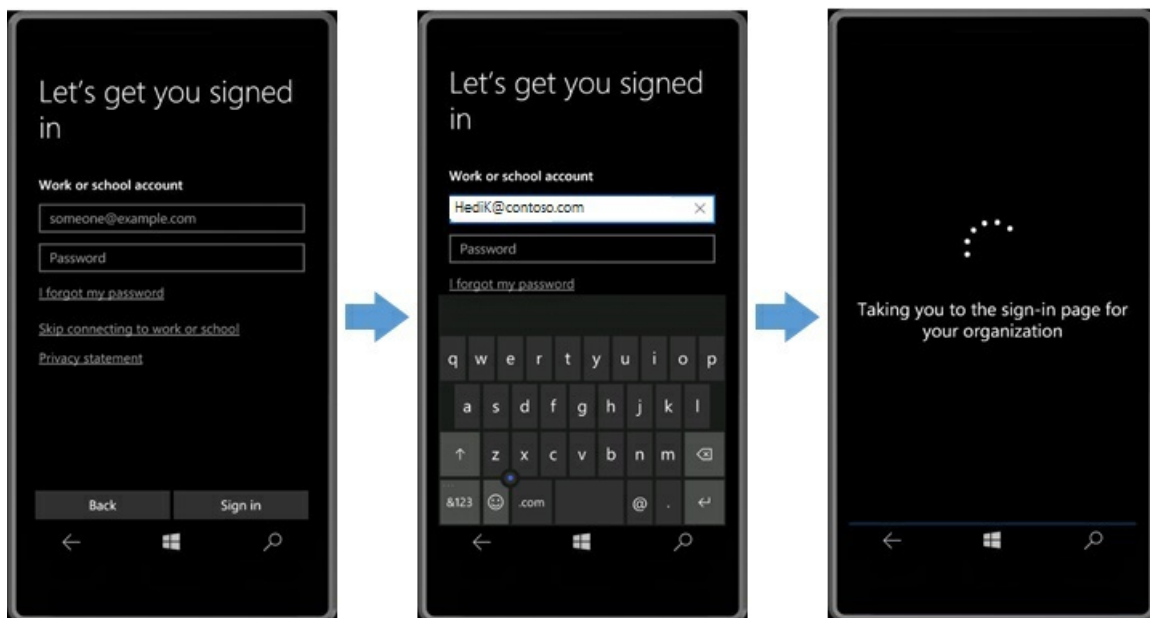
- The apps for **Device backup and restore** and to sync photos to OneDrive only work with the Microsoft account as the primary account—these apps won't work on devices joined to Azure AD.
- **Find my Phone** will work depending on how you add a Microsoft account to the device—for example, the Cortana application will sign in with your Microsoft account in a way that makes **Find my Phone** work. Cortana and OneNote both work with Azure AD accounts but must be set up with a Microsoft account first.
- OneNote requires the user to sign in with a Microsoft account but will also provide access to Notebooks using the Azure AD account.
- If your organization is configured to federate with Azure AD, your federation proxy will need to be Active Directory Federation Services (ADFS) or a 3rd party which supports WS-Trust endpoints just like ADFS does.

How to join Windows 10 Mobile to Azure AD

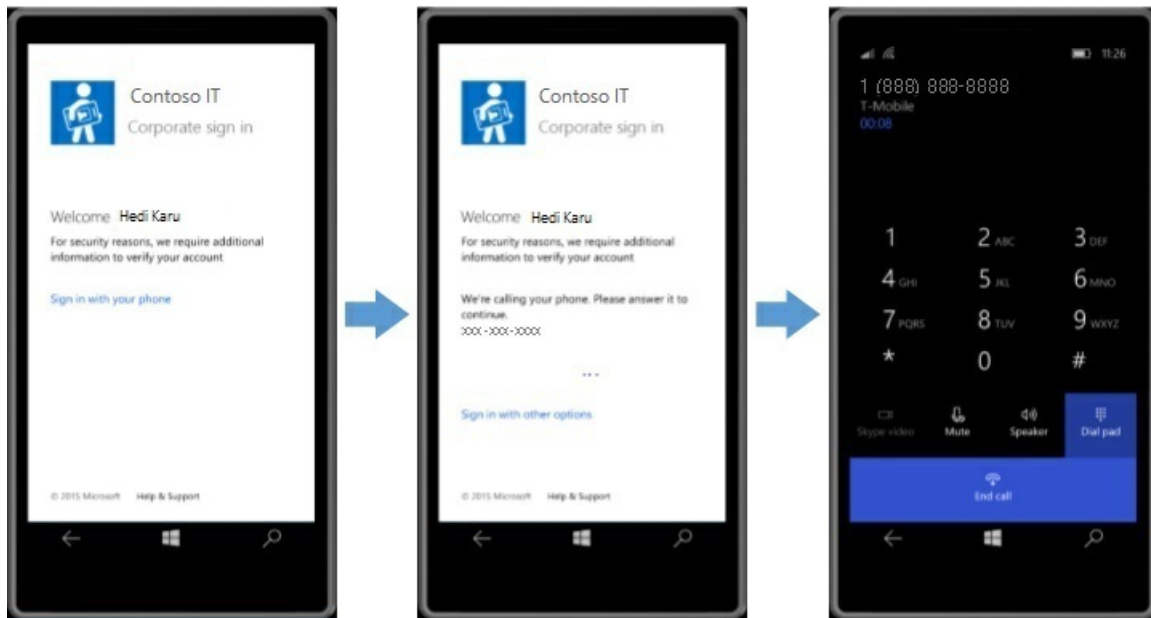
1. During OOB, on the **Keep your life in sync** screen, choose the option **Sign in with a work account**, and then tap **Next**.



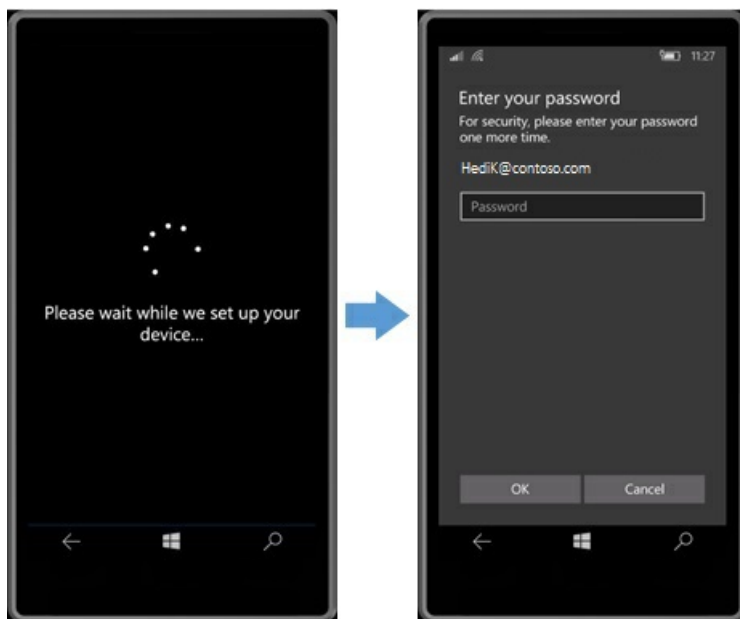
2. Enter your Azure AD account. If your Azure AD account is federated, you will be redirected to your organization's sign-in page; if not, you enter your password here.



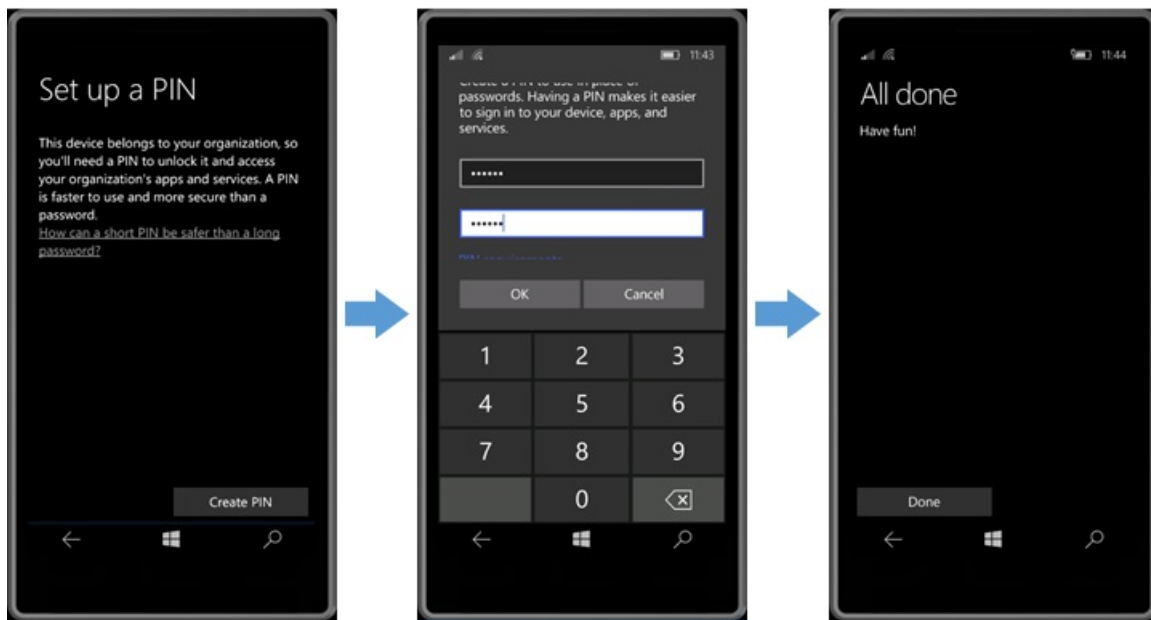
If you are taken to your organization's sign-in page, you may be required to provide a second factor of authentication.



3. After authentication completes, the device registration is complete. If your MDM service has a terms of use page, it would be seen here as well. Federated users are required to provide a password again to complete the authentication to Windows. Users with passwords managed in the cloud will not see this additional authentication prompt. This federated login requires your federation server to support a WS-Trust active endpoint.



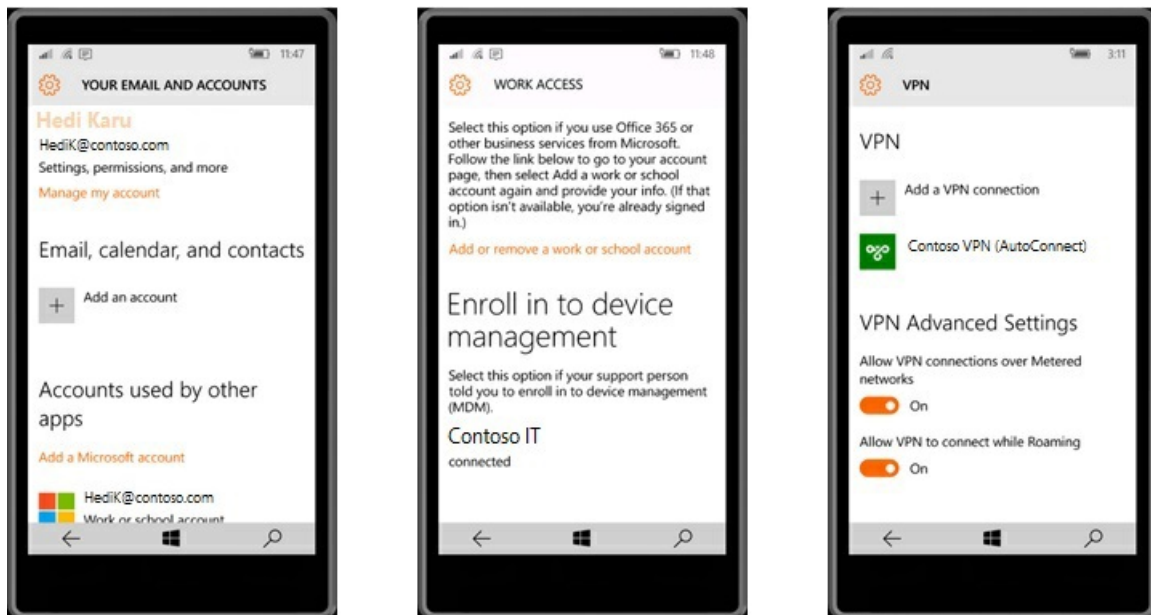
4. Next, you set up a PIN.



Note To learn more about the PIN requirement, see [Why a PIN is better than a password](#).

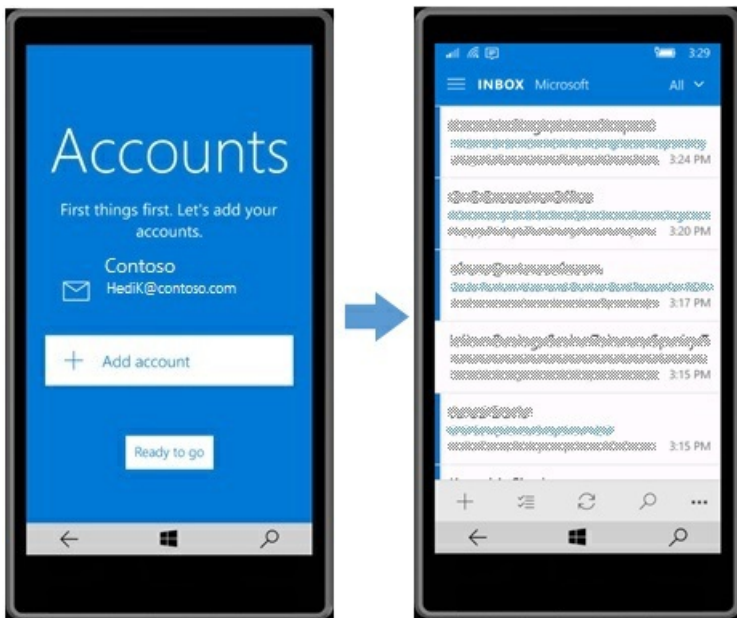
To verify Azure AD join

- Go to **Settings > Accounts > Your email and accounts**. You will see your Azure AD account listed at the top and also listed as an account used by other apps. If auto-enrollment into MDM was configured, you will see in **Settings > Accounts > Work Access** that the device is correctly enrolled in MDM. If the MDM is pushing a certificate to be used by VPN, then **Settings > Network & wireless > VPN** will show the ability to connect to your VPN.

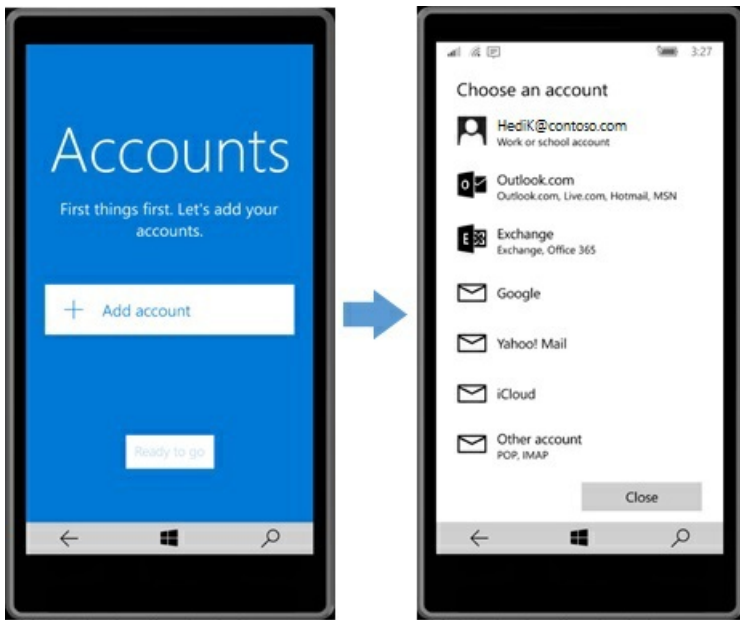


Set up mail and calendar

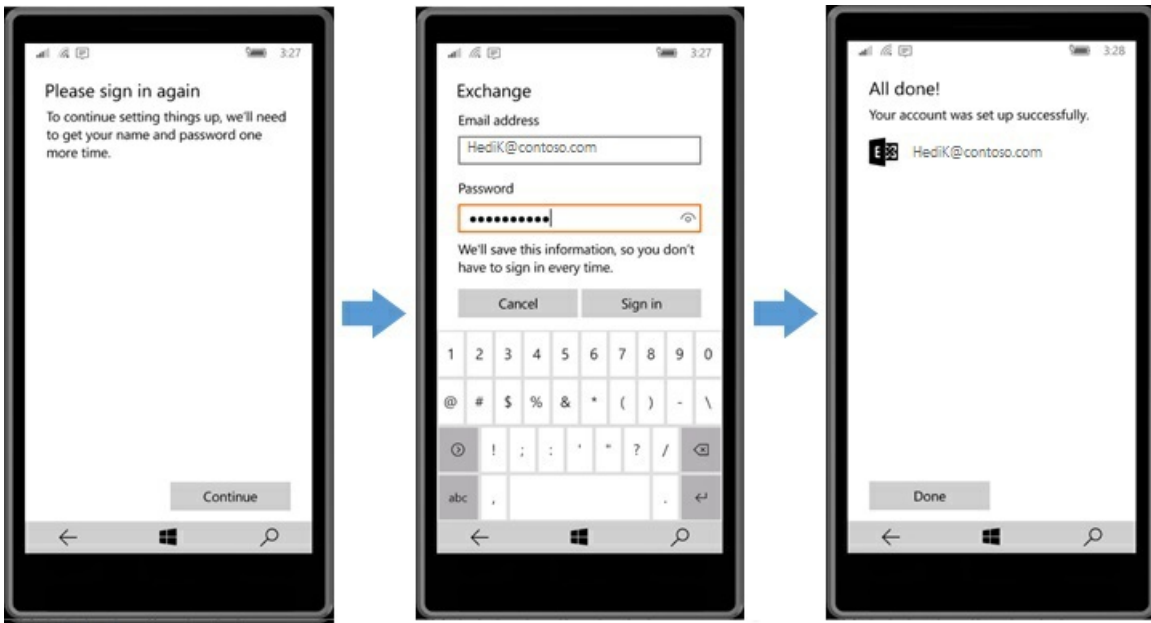
Setting up email on your Azure AD joined device is simple. Launching the **Mail** app brings you to the **Accounts** page. Most users will have their email accounts hosted in Office 365 and will automatically start syncing. Just tap **Ready to go**.



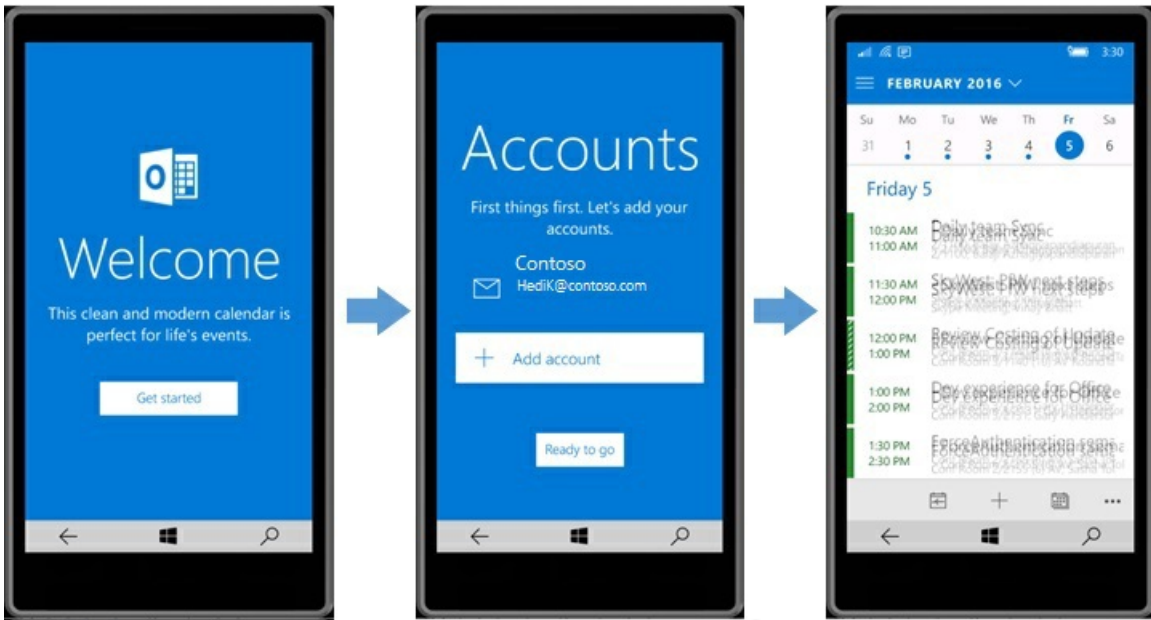
When email is hosted in on-premises Exchange, the user must provide credentials to establish a basic authentication connection to the Exchange server. Tap **Add account** to see the types of mail accounts you can add, including your Azure AD account.



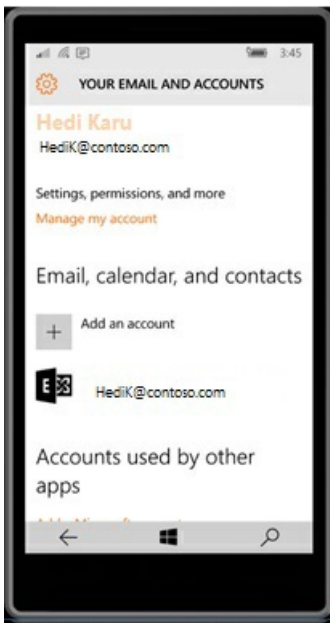
After you select an account type, you provide credentials to complete setup for that mailbox.



Setup for the **Calendar** app is similar. Open the app and you'll see your Azure AD account listed -- just tap **Ready to go**.



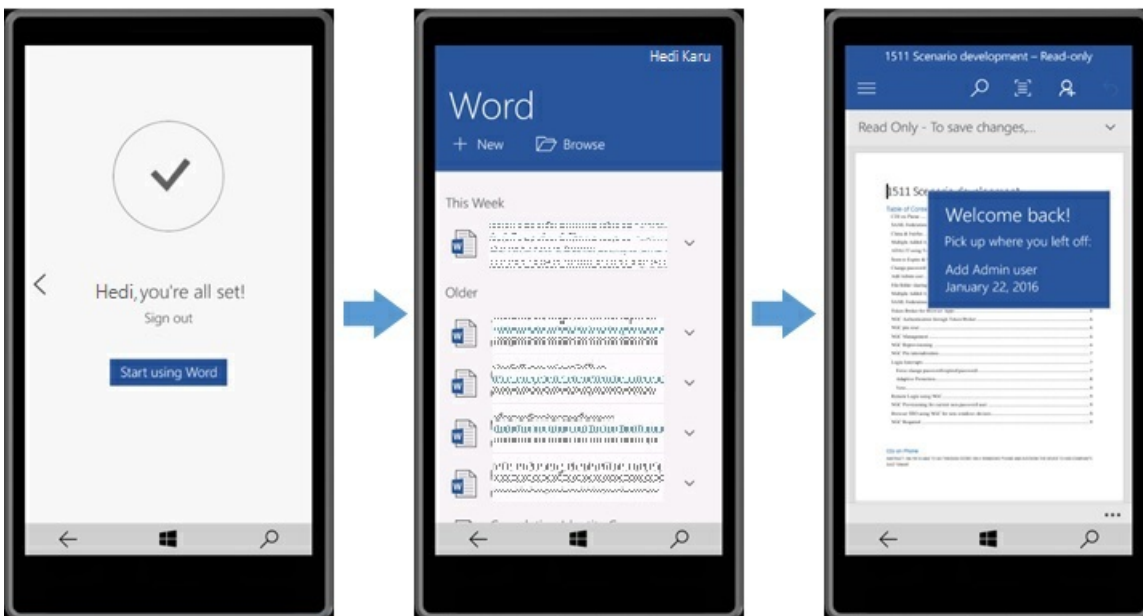
Return to **Settings > Accounts > Your email and accounts**, and you will see your Azure AD account listed for **Email, calendar, and contacts**.



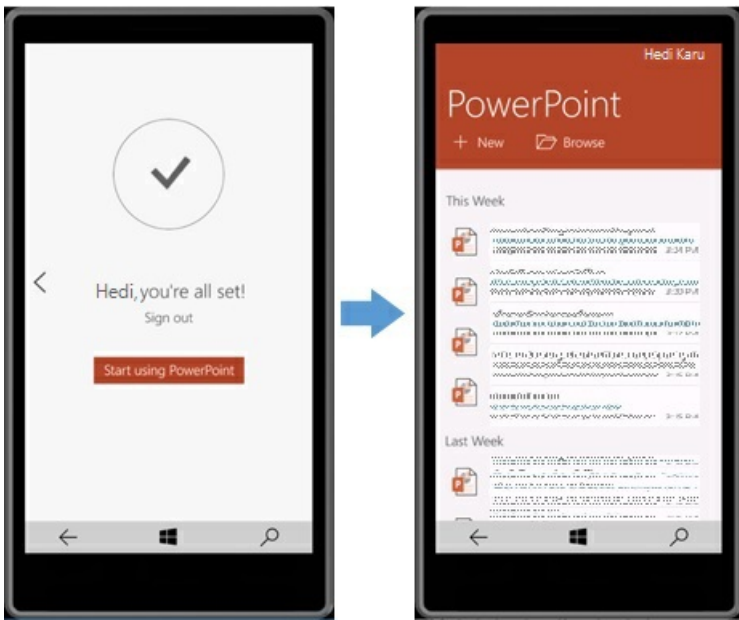
Use Office and OneDrive apps

Office applications like Microsoft Word and Microsoft PowerPoint will automatically sign you in with your Azure AD account. When you open an Office app, you see a screen that allows you to choose between a Microsoft account and Azure AD account. Office shows this screen while it is automatically signing you in, so just be patient for a couple seconds and Office will automatically sign you in using your Azure AD account.

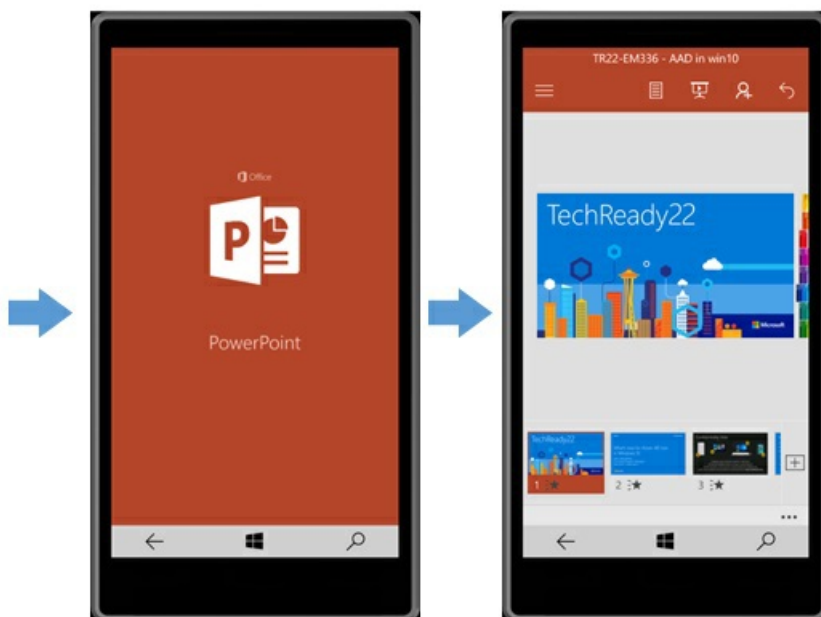
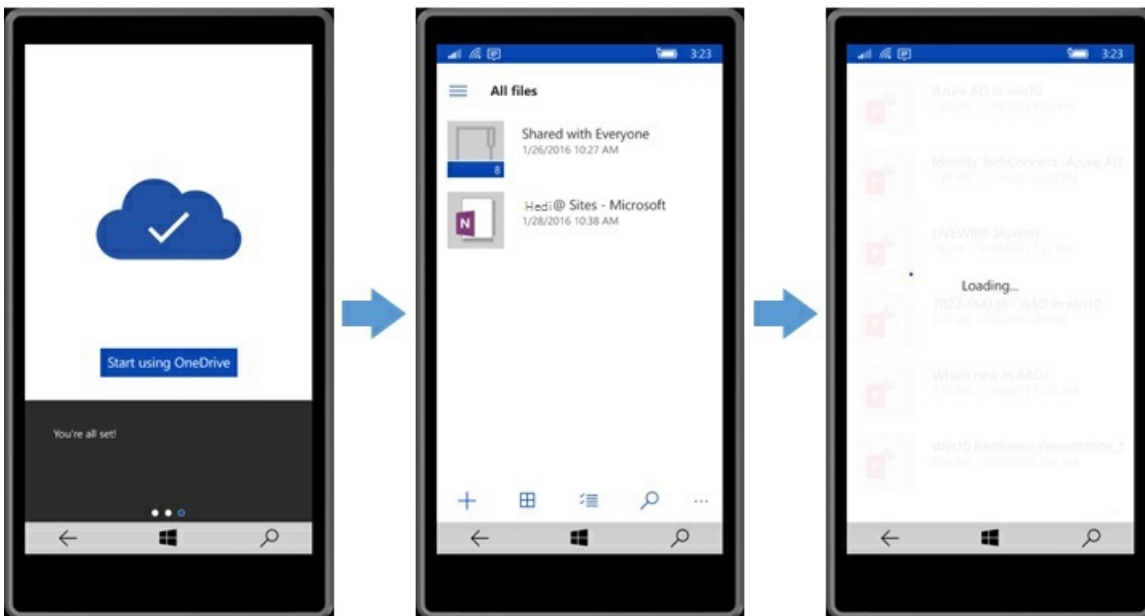
Microsoft Word automatically shows the documents recently opened on other devices. Opening a document allows you to jump straight to the same section you were last editing on another device.



Microsoft PowerPoint shows your recently opened slide decks.

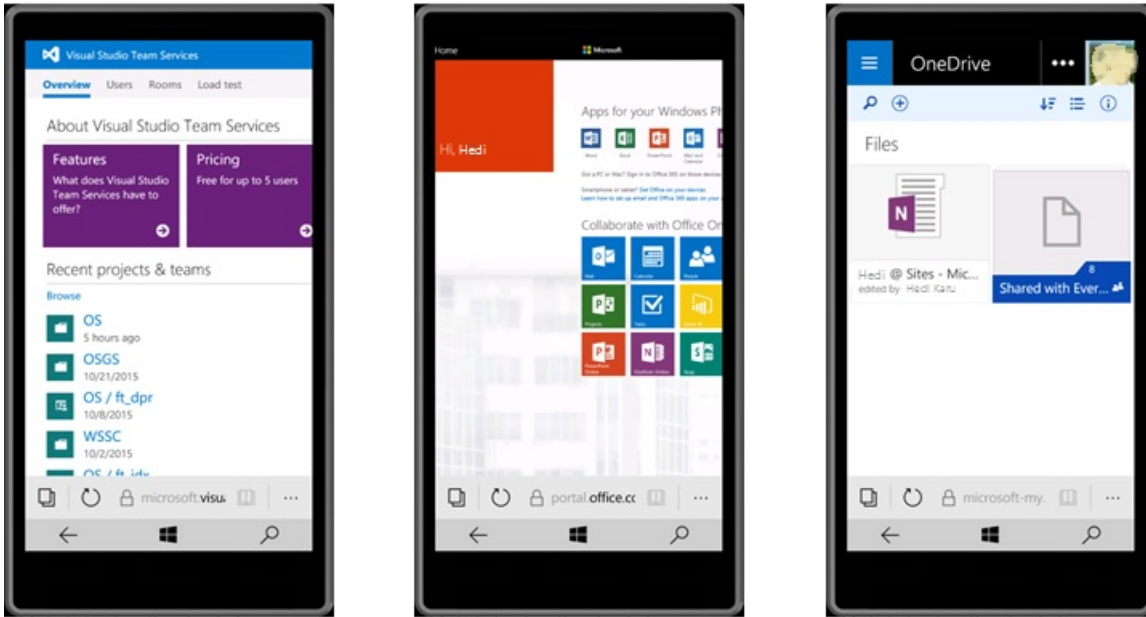


The OneDrive application also uses SSO, showing you all your documents and enabling you to open them without any authentication experience.

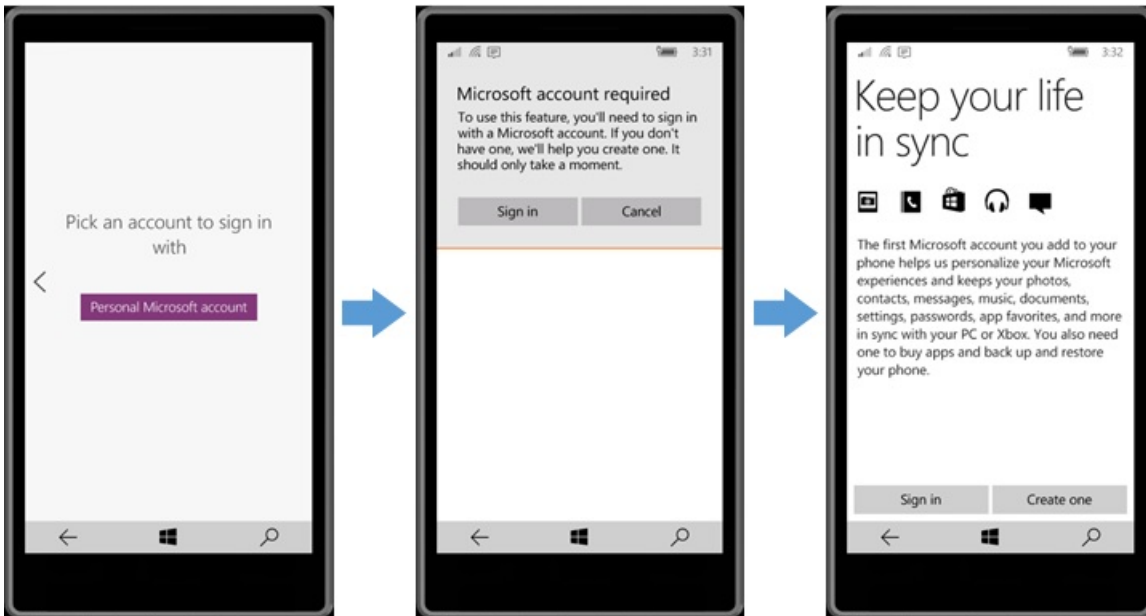


In addition to application SSO, Azure AD joined devices also get SSO for browser applications which trust Azure

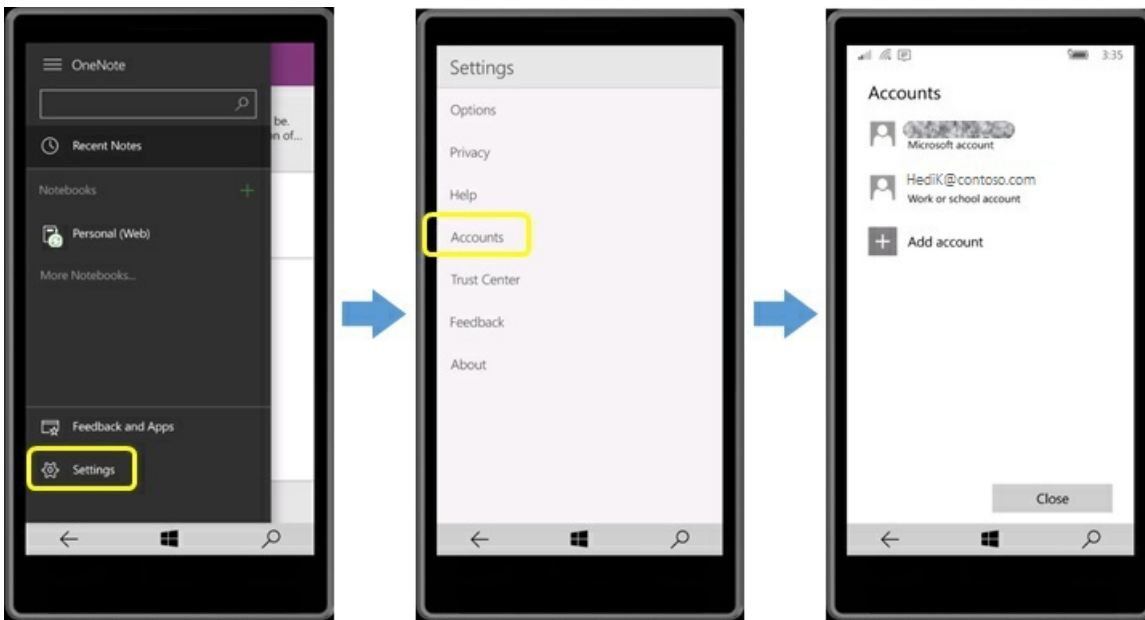
AD, such as web applications, Visual Studio, Office 365 portal, and OneDrive for Business.



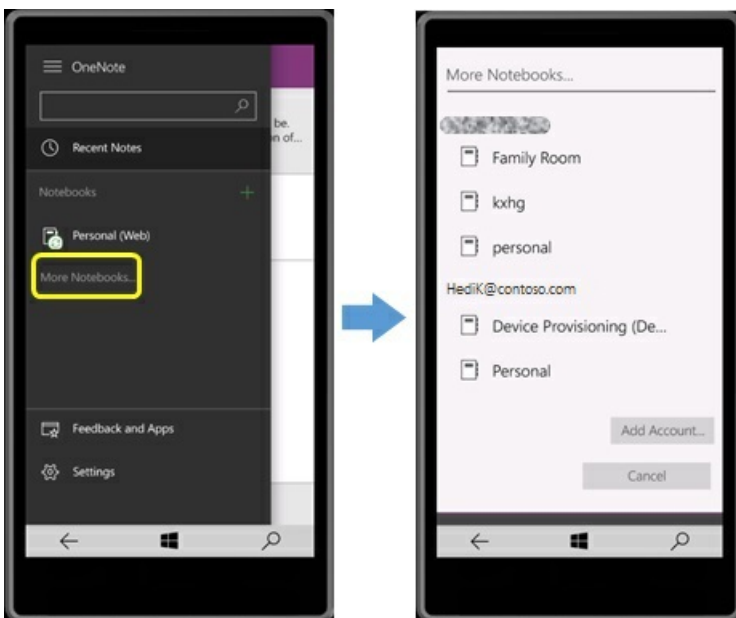
OneNote requires a Microsoft account, but you can use it with your Azure AD account as well.



After you sign in to OneNote, go to Settings > Accounts, and you will see that your Azure AD account is automatically added.

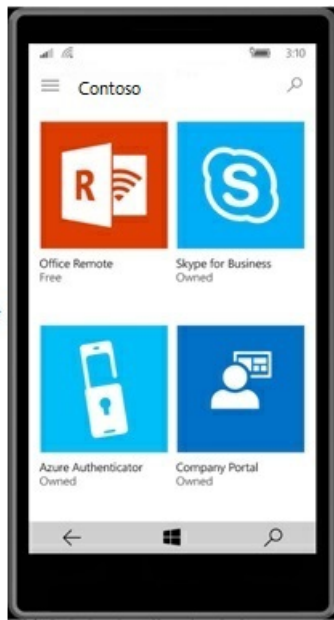
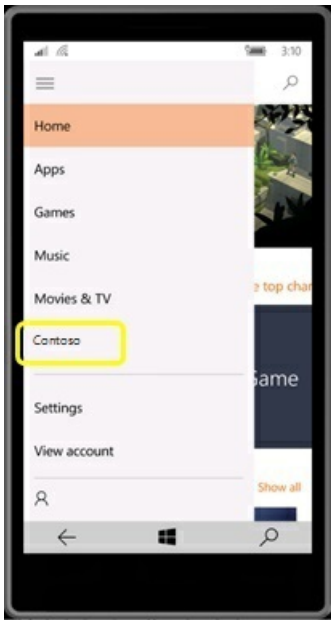


To see the Notebooks that your Azure AD account has access to, tap **More Notebooks** and select the Notebook you want to open.



Use Microsoft Store for Business

[Microsoft Store for Business](#) allows you to specify applications to be available to your users in the Microsoft Store application. These applications show up on a tab titled for your company. Applications approved in the Microsoft Store for Business portal can be installed by users.



New policies for Windows 10

5/31/2019 • 9 minutes to read • [Edit Online](#)

Applies to

- Windows 10
- Windows 10 Mobile

Windows 10 includes the following new policies for management. [Download the complete set of Administrative Template \(.adm\) files for Windows 10.](#)

New Group Policy settings in Windows 10, version 1709

The following Group Policy settings were added in Windows 10, version 1709:

Control Panel

- Control Panel\Allow Online Tips

Network

- Network\Network Connectivity Status Indicator\Specify global DNS
- Network\WWAN Service\WWAN UI Settings\Set Per-App Cellular Access UI Visibility
- Network\WWAN Service\Cellular Data Access\Let Windows apps access cellular data

System

- System\Device Health Attestation Service\Enable Device Health Attestation Monitoring and Reporting
- System\OS Policies\Enables Activity Feed
- System\OS Policies\Allow publishing of User Activities
- System\Power Management\Power Throttling Settings\Turn off Power Throttling
- System\Storage Health\Allow downloading updates to the Disk Failure Prediction Model
- System\Trusted Platform Module Services\Configure the system to clear the TPM if it is not in a ready state.

Windows Components

- Windows Components\App Privacy\Let Windows apps communicate with unpaired devices
- Windows Components\Data Collection and Preview Builds\Limit Enhanced diagnostic data to the minimum required by Windows Analytics
- Windows Components\Handwriting\Handwriting Panel Default Mode Docked
- Windows Components\Internet Explorer\Internet Settings\Advanced settings\Browsing\Hide the button (next to the New Tab button) that opens Microsoft Edge
- Windows Components\MDM\Auto MDM Enrollment with AAD Token
- Windows Components\Messaging\Allow Message Service Cloud Sync
- Windows Components\Microsoft Edge\Always show the Books Library in Microsoft Edge
- Windows Components\Microsoft Edge\Provision Favorites
- Windows Components\Microsoft Edge\Prevent changes to Favorites on Microsoft Edge
- Windows Components\Microsoft FIDO Authentication\Enable usage of FIDO devices to sign on
- Windows Components\OneDrive\Prevent OneDrive from generating network traffic until the user signs in to OneDrive

- Windows Components\Push To Install\Turn off Push To Install service
- Windows Components\Search\Allow Cloud Search
- Windows Components\Windows Defender Application Guard\Allow data persistence for Windows Defender Application Guard
- Windows Components\Windows Defender Application Guard\Allow auditing events in Windows Defender Application Guard
- Windows Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Network Protection\Prevent users and apps from accessing dangerous websites
- Windows Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Controlled Folder Access\Configure Controlled folder access
- Windows Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction rules
- Windows Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Attack Surface Reduction\Exclude files and paths from Attack Surface Reduction Rules
- Windows Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Controlled Folder Access\Configure allowed applications
- Windows Components\Windows Defender Antivirus\Windows Defender Exploit Guard\Controlled Folder Access\Configure protected folders
- Windows Components\Windows Defender Exploit Guard\Exploit Protection\Use a common set of exploit protection settings
- Windows Components\Windows Defender Security Center\Virus and threat protection\Hide the Virus and threat protection area
- Windows Components\Windows Defender Security Center\Firewall and network protection\Hide the Firewall and network protection area
- Windows Components\Windows Defender Security Center\App and browser protection\Hide the App and browser protection area
- Windows Components\Windows Defender Security Center\App and browser protection\Prevent users from modifying settings
- Windows Components\Windows Defender Security Center\Device performance and health\Hide the Device performance and health area
- Windows Components\Windows Defender Security Center\Family options\Hide the Family options area
- Windows Components\Windows Defender Security Center\Notifications\Hide all notifications
- Windows Components\Windows Defender Security Center\Notifications\Hide non-critical notifications
- Windows Components\Windows Defender Security Center\Enterprise Customization\Configure customized notifications
- Windows Components\Windows Defender Security Center\Enterprise Customization\Configure customized contact information
- Windows Components\Windows Defender Security Center\Enterprise Customization\Specify contact company name
- Windows Components\Windows Defender Security Center\Enterprise Customization\Specify contact phone number or Skype ID
- Windows Components\Windows Defender Security Center\Enterprise Customization\Specify contact email address or Email ID
- Windows Components\Windows Defender Security Center\Enterprise Customization\Specify contact website
- Windows Components\Windows Hello for Business\Configure device unlock factors
- Windows Components\Windows Hello for Business\Configure dynamic lock factors
- Windows Components\Windows Hello for Business\Turn off smart card emulation
- Windows Components\Windows Hello for Business\Allow enumeration of emulated smart card for all users

- Windows Components\Windows Update\Allow updates to be downloaded automatically over metered connections
- Windows Components\Windows Update\Do not allow update deferral policies to cause scans against Windows Update

New Group Policy settings in Windows 10, version 1703

The following Group Policy settings were added in Windows 10, version 1703:

Control Panel

- Control Panel\Add or Remove Programs\Specify default category for Add New Programs
- Control Panel\Add or Remove Programs\Hide the "Add a program from CD-ROM or floppy disk" option
- Control Panel\Personalization\Prevent changing lock screen and logon image

Network

- Network\Background Intelligent Transfer Service (BITS)\Limit the maximum network bandwidth for BITS background transfers
- Network\Background Intelligent Transfer Service (BITS)\Allow BITS Peercaching
- Network\Background Intelligent Transfer Service (BITS)\Limit the age of files in the BITS Peercache
- Network\Background Intelligent Transfer Service (BITS)\Limit the BITS Peercache size
- Network\DNS Client\Allow NetBT queries for fully qualified domain names
- Network\Network Connections\Prohibit access to properties of components of a LAN connection
- Network\Network Connections\Ability to Enable/Disable a LAN connection
- Network\Offline Files\Turn on economical application of administratively assigned Offline Files
- Network\Offline Files\Configure slow-link mode
- Network\Offline Files\Enable Transparent Caching
- Network\Microsoft Peer-to-Peer Networking Services\Peer Name Resolution Protocol\Site-Local Clouds\Set the Seed Server
- Network\Microsoft Peer-to-Peer Networking Services\Disable password strength validation for Peer Grouping

System

- System\App-V\Streaming\Location Provider
- System\App-V\Streaming\Certificate Filter For Client SSL
- System\Credentials Delegation\Allow delegating default credentials with NTLM-only server authentication
- System\Ctrl+Alt+Del Options\Remove Change Password
- System\Ctrl+Alt+Del Options\Remove Lock Computer
- System\Ctrl+Alt+Del Options\Remove Task Manager
- System\Ctrl+Alt+Del Options\Remove Logoff
- System\Device Installation\Do not send a Windows error report when a generic driver is installed on a device
- System\Device Installation\Prevent Windows from sending an error report when a device driver requests additional software during installation
- System\Locale Services\Disallow user override of locale settings
- System\Logon\Do not process the legacy run list
- System\Logon\Always use custom logon background
- System\Logon\Do not display network selection UI
- System\Logon\Block user from showing account details on sign-in
- System\Logon\Turn off app notifications on the lock screen
- System\User Profiles\Establish timeout value for dialog boxes

- System\Enable Windows NTP Server\Windows Time Service\Enable Windows NTP Client

Windows Components

- Windows Components\ActiveX Installer Service\Approved Installation Sites for ActiveX Controls
- Windows Components\ActiveX Installer Service\Establish ActiveX installation policy for sites in Trusted zones
- Windows Components\Application Compatibility\Turn off Application Compatibility Engine
- Windows Components\Application Compatibility\Turn off Program Compatibility Assistant
- Windows Components\Application Compatibility\Turn off Steps Recorder
- Windows Components\Attachment Manager\Notify antivirus programs when opening attachments
- Windows Components\Biometrics\Allow the use of biometrics
- Windows Components\NetMeeting\Disable Whiteboard
- Windows Components\Data Collection and Preview Builds\Configurate the Commercial ID
- Windows Components\File Explorer\Display the menu bar in File Explorer
- Windows Components\File History\Turn off File History
- Windows Components\Internet Explorer\Internet Control Panel\Advanced Page\Play animations in web pages
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Trusted Sites Zone\Turn on Cross-Site Scripting Filter
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Turn on Cross-Site Scripting Filter
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Internet Zone\Run ActiveX controls and plugins
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Internet Zone\Script ActiveX controls marked safe for scripting
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Intranet Zone\Run ActiveX controls and plugins
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Intranet Zone\Script ActiveX controls marked safe for scripting
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Intranet Zone\Run ActiveX controls and plugins
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Intranet Zone\Script ActiveX controls marked safe for scripting
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Local Machine Zone\Run ActiveX controls and plugins
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Local Machine Zone\Script ActiveX controls marked safe for scripting
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Local Machine Zone\Run ActiveX controls and plugins
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Local Machine Zone\Script ActiveX controls marked safe for scripting
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Run ActiveX controls and plugins
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Script ActiveX controls marked safe for scripting
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Restricted Sites Zone\Run ActiveX controls and plugins
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Restricted Sites Zone\Script ActiveX controls marked safe for scripting
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Trusted Sites Zone\Run ActiveX

controls and plugins

- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Trusted Sites Zone\Script ActiveX controls marked safe for scripting
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Trusted Sites Zone\Run ActiveX controls and plugins
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Trusted Sites Zone\Script ActiveX controls marked safe for scripting
- Windows Components\Internet Explorer\Accelerators\Restrict Accelerators to those deployed through Group Policy
- Windows Components\Internet Explorer\Compatibility View\Turn on Internet Explorer 7 Standards Mode
- Windows Components\Location and Sensors\Windows Location Provider\Turn off Windows Location Provider
- Windows Components\Microsoft Account\Block all consumer Microsoft account user authentication
- Windows Components\Microsoft Edge\Configure Autofill
- Windows Components\Microsoft Edge\Allow Developer Tools
- Windows Components\Microsoft Edge\Configure Do Not Track
- Windows Components\Microsoft Edge\Allow InPrivate browsing
- Windows Components\Microsoft Edge\Configure Password Manager
- Windows Components\Microsoft Edge\Configure Pop-up Blocker
- Windows Components\Microsoft Edge\Allow search engine customization
- Windows Components\Microsoft Edge\Configure search suggestions in Address bar
- Windows Components\Microsoft Edge\Set default search engine
- Windows Components\Microsoft Edge\Configure additional search engines
- Windows Components\Microsoft Edge\Configure the Enterprise Mode Site List
- Windows Components\Microsoft Edge\Prevent using Localhost IP address for WebRTC
- Windows Components\Microsoft Edge\Configure Start pages
- Windows Components\Microsoft Edge\Disable lockdown of Start pages
- Windows Components\Microsoft Edge\Prevent bypassing Windows Defender SmartScreen prompts for sites
- Windows Components\Microsoft Edge\Prevent bypassing Windows Defender SmartScreen prompts for files
- Windows Components\Microsoft Management Console\Restricted/Permitted snap-ins.Net Framework Configuration
- Windows Components\Windows Installer\Prohibit use of Restart Manager
- Windows Components\Desktop Gadgets\Restrict unpacking and installation of gadgets that are not digitally signed.
- Windows Components\Desktop Gadgets\Turn Off user-installed desktop gadgets
- Windows Components\OneDrive\Prevent the usage of OneDrive for file storage
- Windows Components\OneDrive\Prevent the usage of OneDrive for file storage on Windows 8.1
- Windows Components\OneDrive\Prevent OneDrive files from syncing over metered connections
- Windows Components\OneDrive\Save documents to OneDrive by default
- Windows Components\Smart Card\Allow certificates with no extended key usage certificate attribute
- Windows Components\Smart Card\Turn on certificate propagation from smart card
- Windows Components\Tablet PC\Pen UX Behaviors\Prevent flicks
- Windows Components\BitLocker Drive Encryption\Choose drive encryption method and cipher strength (Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10 [Version 1507])
- Windows Components\Windows Defender Antivirus\Real-time Protection\Turn on behavior monitoring
- Windows Components\Windows Defender Antivirus\Signature Updates\Define file shares for downloading definition updates

- Windows Components\Windows Defender Antivirus\Signature Updates\Turn on scan after signature update
- Windows Components\File Explorer\Display confirmation dialog when deleting files
- Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Restricted Sites Zone\Allow OpenSearch queries in File Explorer
- Windows Components\Windows Update\Remove access to use all Windows Update features
- Windows Components\Windows Update\Configure Automatic Updates
- Windows Components\Windows Update\Specify intranet Microsoft update service location
- Windows Components\Windows Update\Automatic Updates detection frequency
- Windows Components\Windows Update\Allow non-administrators to receive update notifications
- Windows Components\Windows Update\Allow Automatic Updates immediate installation
- Windows Components\Windows Update\Turn on recommended updates via Automatic Updates
- Windows Components\Shutdown Options\Turn off legacy remote shutdown interface

For a spreadsheet of Group Policy settings included in Windows 10 and Windows Server 2016, see [Group Policy Settings Reference for Windows and Windows Server](#).

New MDM policies

Mobile device management (MDM) for Windows 10 Pro, Windows 10 Enterprise, Windows 10 Education, and Windows 10 Mobile includes settings from Windows Phone 8.1, plus new or enhanced settings for Windows 10, such as:

- Defender (Windows 10 Pro, Windows 10 Enterprise, and Windows 10 Education only)
- Enhanced Bluetooth policies
- Passport and Hello
- Device update
- Hardware-based device health attestation
- [Kiosk mode](#), start screen, start menu layout
- Security
- [VPN](#) and enterprise Wi-Fi management
- Certificate management
- Windows Tips
- Consumer experiences, such as suggested apps in Start and app tiles from Microsoft dynamically inserted in the default Start menu

Windows 10, version 1703, adds a number of [ADMX-backed policies to MDM](#).

If you use Microsoft Intune for MDM, you can [configure custom policies](#) to deploy Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings that can be used to control features on Windows 10. For a list of OMA-URI settings, see [Custom URI settings for Windows 10 devices](#).

No new [Exchange ActiveSync policies](#). For more information, see the [ActiveSync configuration service provider](#) technical reference.

Related topics

[Group Policy Settings Reference Spreadsheet Windows 1803](#)

[Manage corporate devices](#)

[Changes to Group Policy settings for Start in Windows 10](#)

[Windows 10 Mobile and MDM](#)

Group Policy settings that apply only to Windows 10 Enterprise and Education Editions

5/31/2019 • 2 minutes to read • [Edit Online](#)

Applies to

- Windows 10

In Windows 10, version 1607, the following Group Policy settings apply only to Windows 10 Enterprise and Windows 10 Education.

POLICY NAME	POLICY PATH	COMMENTS
Configure Spotlight on lock screen	User Configuration > Administrative Templates > Windows Components > Cloud Content	For more info, see Windows spotlight on the lock screen . Note that an additional Cloud Content policy, Do not suggest third-party content in Windows spotlight , does apply to Windows 10 Pro.
Turn off all Windows Spotlight features	User Configuration > Administrative Templates > Windows Components > Cloud Content	For more info, see Windows spotlight on the lock screen
Turn off Microsoft consumer features	Computer Configuration > Administrative Templates > Windows Components > Cloud Content	For more info, see Windows spotlight on the lock screen
Do not display the lock screen	Computer Configuration > Administrative Templates > Control Panel > Personalization	For more info, see Windows spotlight on the lock screen
Do not require CTRL+ALT+DEL combined with Turn off app notifications on the lock screen	Computer Configuration > Administrative Templates > System > Logon and Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Interactive logon	When both of these policy settings are enabled, the combination will also disable lock screen apps (assigned access) on Windows 10 Enterprise and Windows 10 Education only. These policy settings can be applied to Windows 10 Pro, but lock screen apps will not be disabled on Windows 10 Pro. Important: The description for Interactive logon: Do not require CTRL+ALT+DEL in the Group Policy Editor incorrectly states that it only applies to Windows 10 Enterprise and Education. The description will be corrected in a future release.
Do not show Windows Tips	Computer Configuration > Administrative Templates > Windows Components > Cloud Content	For more info, see Windows spotlight on the lock screen

POLICY NAME	POLICY PATH	COMMENTS
Force a specific default lock screen image	Computer Configuration > Administrative Templates > Control Panel > Personalization	For more info, see Windows spotlight on the lock screen
Start layout	User Configuration\Administrative Templates\Start Menu and Taskbar	In Windows 10, version 1703, this policy setting can be applied to Windows 10 Pro. For more info, see Manage Windows 10 Start layout options and policies
Turn off the Store application	<p>Computer Configuration > Administrative Templates > Windows Components > Store > Turn off the Store application</p> <p>User Configuration > Administrative Templates > Windows Components > Store > Turn off the Store application</p>	For more info, see Knowledge Base article# 3135657 .
Only display the private store within the Microsoft Store app	<p>Computer Configuration > Administrative Templates > Windows Components > Store > Only display the private store within the Microsoft Store app</p> <p>User Configuration > Administrative Templates > Windows Components > Store > Only display the private store within the Microsoft Store app</p>	For more info, see Manage access to private store
Don't search the web or display web results	Computer Configuration\Administrative Templates\Windows Components\Search\Don't search the web or display web results	For more info, see Cortana integration in your enterprise

Applies to

- Windows 10, Windows Server 2016

Manage the Settings app with Group Policy

You can now manage the pages that are shown in the Settings app by using Group Policy. This lets you hide specific pages from users. Before Windows 10, version 1703, you could either show everything in the Settings app or hide it completely. To make use of the Settings App group policies on Windows server 2016, install fix [4457127](#) or a later cumulative update.

NOTE

Each server that you want to manage access to the Settings App must be patched.

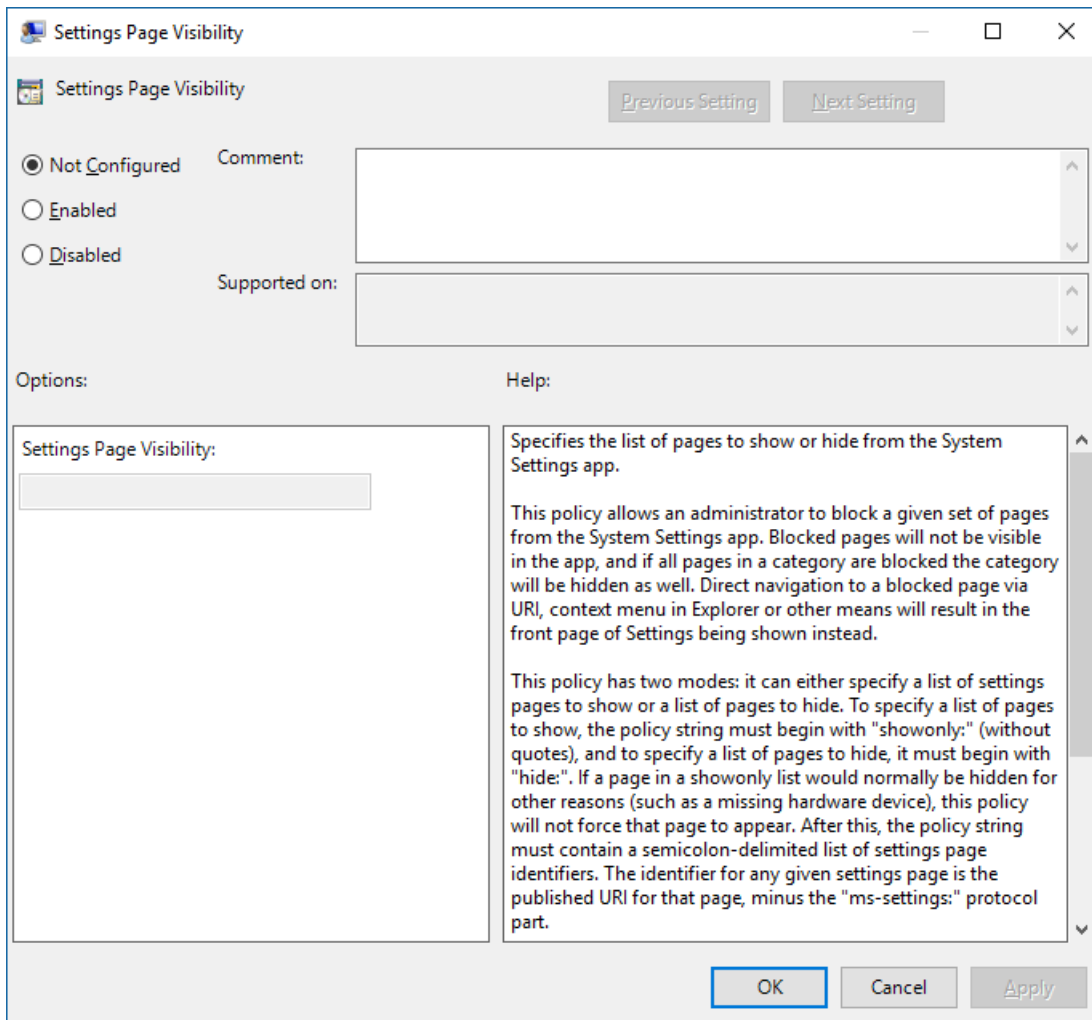
To centrally manage the new policies copy the ControlPanel.admx and ControlPanel.adml file to [Central Store](#) if your company uses one or the PolicyDefinitions folder of the Domain Controllers used for Group Policy management.

This policy is available for both User and Computer depending on the version of the OS. Windows Server 2016 with KB 4457127 applied will have both User and Computer policy. Windows 10, version 1703, added Computer policy for the Settings app. Windows 10, version 1809, added User policy for the Settings app.

Policy paths:

Computer Configuration > Administrative Templates > Control Panel > Settings Page Visibility.

User Configuration > Administrative Templates > Control Panel > Settings Page Visibility.



Configuring the Group Policy

The Group Policy can be configured in one of two ways: specify a list of pages that are shown or specify a list of pages to hide. To do this, add either **ShowOnly:** or **Hide:** followed by a semicolon delimited list of URIs in **Settings Page Visibility**. For a full list of URIs, see the URI scheme reference section in [Launch the Windows Settings app](#).

NOTE

When you specify the URI in the Settings Page Visibility textbox, don't include **ms-settings:** in the string.

Here are some examples:

- To show only the Ethernet and Proxy pages, set the **Settings App Visibility** textbox to **ShowOnly:Network-Proxy;Network-Ethernet**.
- To hide the Ethernet and Proxy pages, set the **Settings App Visibility** textbox to **Hide:Network-Proxy;Network-Ethernet**.

What version of Windows am I running?

5/31/2019 • 2 minutes to read • [Edit Online](#)

To determine if your device is enrolled in the [Long-Term Servicing Channel](#) (LTSC, formerly LTSB) or the [Semi-Annual Channel](#) (SAC) you'll need to know what version of Windows 10 you're running. There are a few ways to figure this out. Each method provides a different set of details, so it's useful to learn about all of them.

System Properties

Click **Start** > **Settings** > **System** > click **About** from the bottom of the left-hand menu

You'll now see **Edition**, **Version**, and **OS Build** information. Something like this:

The image shows two overlapping windows from Windows 10. The 'About Windows' window on the left displays the Windows 10 logo and the following text: 'Microsoft Windows Version 10.0 (Build 10240) © 2015 Microsoft Corporation. All rights reserved. The Windows 10 Enterprise 2015 LTSB operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions. This product is licensed under the Microsoft Software License Terms to: Local_User'. The 'System' window on the right shows system information. A table lists items and values: OS Name (Microsoft Windows 10 Enterprise 2015 LTSB), Version (10.0.10240 Build 10240), Other OS Description (Not Available), OS Manufacturer (Microsoft Corporation), System Name, System Manufacturer, System Model, System Type, System SKU, Processor, and BIOS Version/Date. Below the table, the 'System' section shows 'Windows edition' as 'Windows 10 Enterprise 2015 LTSB' and '© 2015 Microsoft Corporation. All rights reserved.' Other system details include Processor (Intel(R) Core(TM) i7-6820HQ CPU @ 2.70GHz 2.71 GHz), Installed memory (RAM) (3.95 GB (1.13 GB usable)), System type (64-bit Operating System, x64-based processor), and Pen and Touch (Pen and Limited Touch Support with 10 Touch Points).

Using Keyword Search

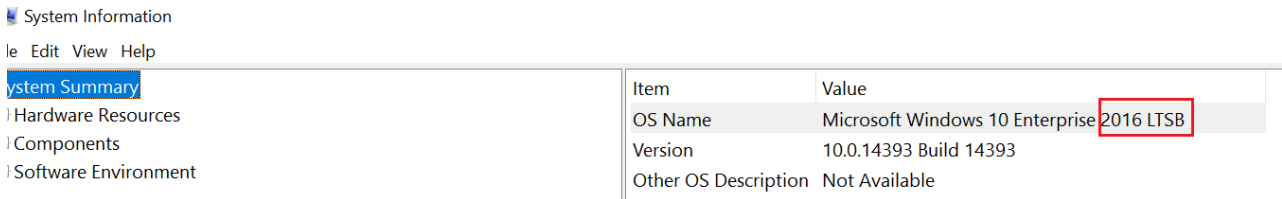
You can simply type the following in the search bar and press **ENTER** to see version details for your device.

“winver”

About Windows

The image shows the search results for 'winver'. At the top is the Windows 10 logo. Below it, the text reads: 'Microsoft Windows Version 1607 (OS Build 14393.0) © 2016 Microsoft Corporation. All rights reserved. The Windows 10 Enterprise 2016 LTSB operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.'

"msinfo" or "msinfo32" to open **System Information**:

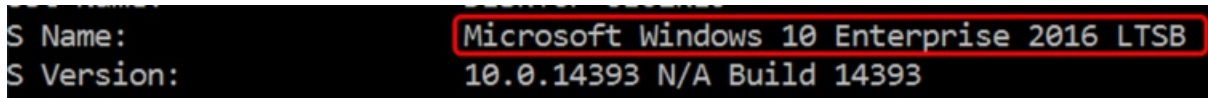


The screenshot shows the System Information application window. The 'System Summary' tab is selected. A table lists system information:

Item	Value
OS Name	Microsoft Windows 10 Enterprise 2016 LTSB
Version	10.0.14393 Build 14393
Other OS Description	Not Available

Using Command Prompt or PowerShell

At the Command Prompt or PowerShell interface, type "**systeminfo | findstr /B /C:"OS Name" /B /C:"OS Version"**" and then press **ENTER**



```
S Name: Microsoft Windows 10 Enterprise 2016 LTSB
S Version: 10.0.14393 N/A Build 14393
```

At the Command Prompt or PowerShell, type "**slmgr /dlv**", and then press ENTER. The /dlv command displays the detailed licensing information. Notice the output displays "EnterpriseS" as seen in the image below:



What does it all mean?

The Long-term Servicing Channel is available only in the Windows 10 Enterprise LTSB edition. This build of Windows doesn't contain many in-box applications, such as Microsoft Edge, Microsoft Store, Cortana (you do have some limited search capabilities), Microsoft Mail, Calendar, OneNote, Weather, News, Sports, Money, Photos, Camera, Music, and Clock. It's important to remember that the LTSC model is primarily for specialized devices.

In the Semi-Annual Channel, you can set feature updates as soon as Microsoft releases them. This servicing modal is ideal for pilot deployments and to test Windows 10 feature updates and for users like developers who need to work with the latest features immediately. Once you've tested the latest release, you can choose when to roll it out broadly in your deployment.

Reset a Windows 10 Mobile device

5/31/2019 • 2 minutes to read • [Edit Online](#)

Applies to

- Windows 10 Mobile

There are two methods for resetting a Windows 10 Mobile device: factory reset and "wipe and persist" reset.

- **Factory reset** restores the state of the device back to its first-boot state plus any update packages. The reset will not return device to the original factory state. To return the device to the original factory state, you must flash it with the original factory image by using the [Windows Device Recovery Tool](#). All the provisioning applied to the device by the enterprise will be lost and will need to be re-applied if needed. For details on what is removed or persists, see [Resetting a mobile device](#).
- **"Wipe and persist" reset** preserves all the provisioning applied to the device before the reset. After the "wipe and persist" reset, all the preserved provisioning packages are automatically applied on the device and the data in the enterprise shared storage folder `\Data\SharedData\Enterprise\Persistent` is restored in that folder. For more information on the enterprise shared storage folder, see [EnterpriseExtFileSystem CSP](#).

You can trigger a reset using your mobile device management (MDM) service, or a user can trigger a reset in the user interface (UI) or by using hardware buttons.

Reset using MDM

The remote wipe command is sent as an XML provisioning file to the device. Since the [RemoteWipe configuration service provider \(CSP\)](#) uses OMA DM and WAP, authentication between client and server and delivery of the XML provisioning file is handled by provisioning. The remote wipe command is implemented on the device by using the **ResetPhone** function. For more information about the data that is removed as a result of the remote wipe command, see [Resetting a mobile device](#).

To perform a factory reset, restoring the device back to its out-of-box state, use the following syncML.

```
<SyncML xmlns="SYNCML:SYNCML1.2">
  <SyncBody>
    <Exec>
      <CmdID>3</CmdID>
      <Item>
        <Target><LocURI>./Vendor/MSFT/RemoteWipe/DoWipe</LocURI></Target>
      </Item>
    </Exec>
  </SyncBody>
</SyncML>
```

To perform a "wipe and persist" reset, preserving the provisioning applied to the device before the reset and persisting data files locally, use the following syncML.

```
<SyncML xmlns="SYNCML:SYNCML1.2">
  <SyncBody>
    <Exec>
      <CmdID>3</CmdID>
      <Item>
        <Target><LocURI>./Vendor/MSFT/RemoteWipe/DoWipePersistProvisionedData</LocURI></Target>
      </Item>
    </Exec>
    <Final/>
  </SyncBody>
</SyncML>
```

Reset using the UI

1. On your mobile device, go to **Settings > System > About > Reset your Phone**
2. When you tap **Reset your phone**, the dialog box will present an option to **Also remove provisioned content** if:
 - At least one provisioning package has been applied, or
 - A file is present in the enterprise shared storage folder `\Data\SharedData\Enterprise\Persistent`.

If the option to **Also remove provisioned content** is selected, the reset that ensues is a regular factory reset. If the option is not selected, a "wipe and persist" reset is performed.

Reset using hardware buttons

If your phone is unresponsive and you can't reach **Settings**, you may be able to reset your phone using the hardware buttons. Reset using hardware buttons does not give you the option to persist provisioned content. On Lumia phones (and some others), do the following to reset your phone:

1. Press and hold the **Volume down** and **Power** buttons at the same time until you feel a vibration (about 10–15 seconds).
2. When you feel the vibration, release the buttons, and then immediately press and hold the **Volume down** button until you see a large exclamation mark.
3. When the exclamation mark appears, press the following four buttons in this order: **Volume up, Volume down, Power, Volume down**. Your phone should now reset and restart itself. (It might take a while for the reset to finish.)

Manage Windows 10 in your organization - transitioning to modern management

5/31/2019 • 9 minutes to read • [Edit Online](#)

Use of personal devices for work, as well as employees working outside the office, may be changing how your organization manages devices. Certain parts of your organization might require deep, granular control over devices, while other parts might seek lighter, scenario-based management that empowers the modern workforce. Windows 10 offers the flexibility to respond to these changing requirements, and can easily be deployed in a mixed environment. You can shift the percentage of Windows 10 devices gradually, following the normal upgrade schedules used in your organization.

Your organization might have considered bringing in Windows 10 devices and downgrading them to Windows 7 until everything is in place for a formal upgrade process. While this may appear to save costs due to standardization, greater savings can come from avoiding the downgrade and immediately taking advantage of the cost reductions Windows 10 can provide. Because Windows 10 devices can be managed using the same processes and technology as other previous Windows versions, it's easy for versions to coexist.

Your organization can support various operating systems across a wide range of device types, and manage them through a common set of tools such as System Center Configuration Manager, Microsoft Intune, or other third-party products. This "managed diversity" enables you to empower your users to benefit from the productivity enhancements available on their new Windows 10 devices (including rich touch and ink support), while still maintaining your standards for security and manageability. It can help you and your organization benefit from Windows 10 much faster.

This six-minute video demonstrates how users can bring in a new retail device and be up and working with their personalized settings and a managed experience in a few minutes, without being on the corporate network. It also demonstrates how IT can apply policies and configurations to ensure device compliance.

NOTE

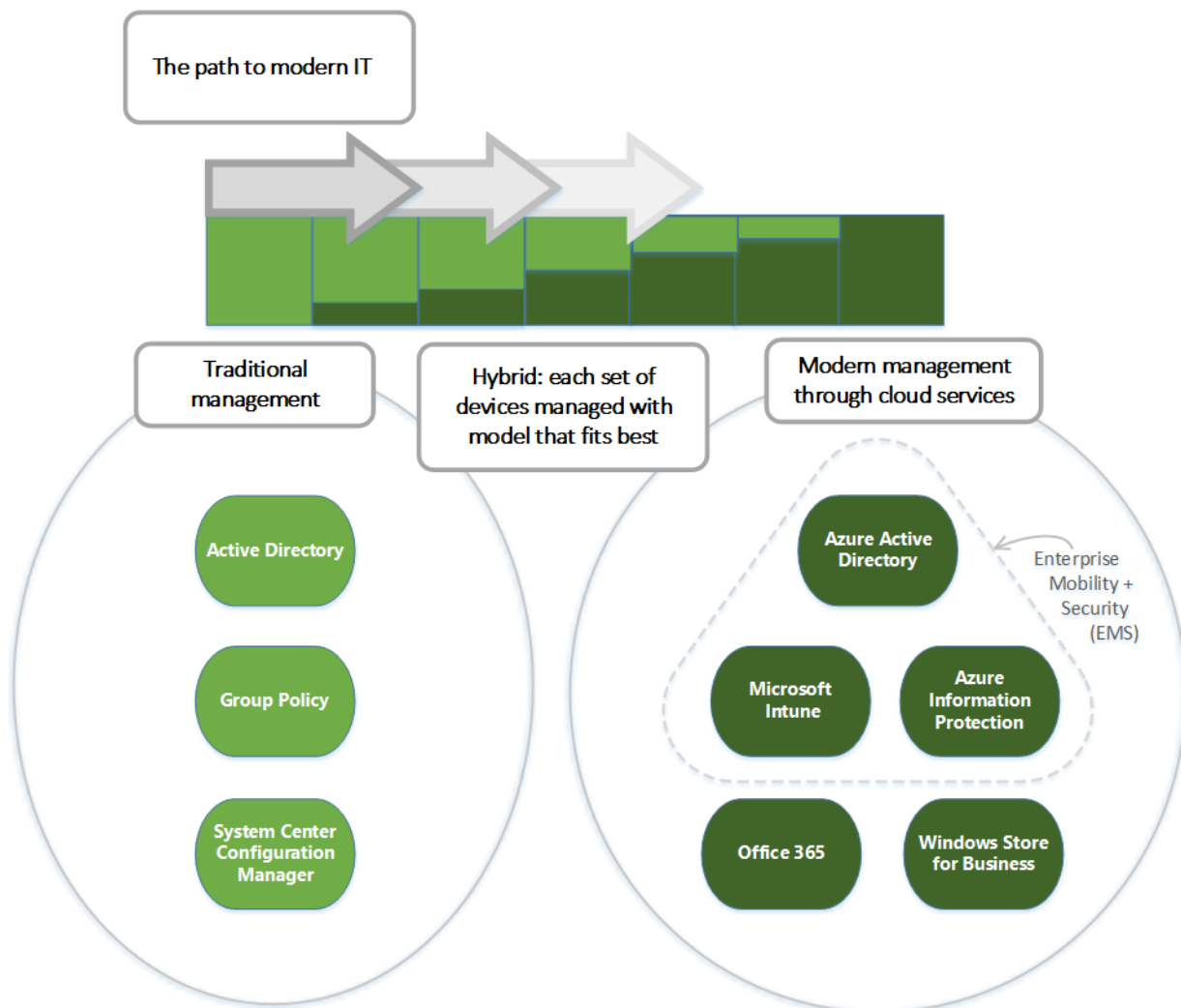
The video demonstrates the configuration process using the classic Azure portal, which is retired. Customers should use the new Azure portal. [Learn how use the new Azure portal to perform tasks that you used to do in the classic Azure portal.](#)

This topic offers guidance on strategies for deploying and managing Windows 10, including deploying Windows 10 in a mixed environment. The topic covers [management options](#) plus the four stages of the device lifecycle:

- [Deployment and Provisioning](#)
- [Identity and Authentication](#)
- [Configuration](#)
- [Updating and Servicing](#)

Reviewing the management options with Windows 10

Windows 10 offers a range of management options, as shown in the following diagram:



As indicated in the diagram, Microsoft continues to provide support for deep manageability and security through technologies like Group Policy, Active Directory, and System Center Configuration Manager. It also delivers a “mobile-first, cloud-first” approach of simplified, modern management using cloud-based device management solutions such as Microsoft Enterprise Mobility + Security (EMS). Future Windows innovations, delivered through Windows as a Service, are complemented by cloud services like Microsoft Intune, Azure Active Directory, Azure Information Protection, Office 365, and the Microsoft Store for Business.

Deployment and Provisioning

With Windows 10, you can continue to use traditional OS deployment, but you can also “manage out of the box.” To transform new devices into fully-configured, fully-managed devices, you can:

- Avoid reimaging by using dynamic provisioning, enabled by a cloud-based device management services such as [Microsoft Autopilot](#) or [Microsoft Intune](#).
- Create self-contained provisioning packages built with the [Windows Configuration Designer](#).
- Use traditional imaging techniques such as deploying custom images using [System Center Configuration Manager](#).

You have multiple options for [upgrading to Windows 10](#). For existing devices running Windows 7 or Windows 8.1, you can use the robust in-place upgrade process for a fast, reliable move to Windows 10 while automatically preserving all the existing apps, data, and settings. This can mean significantly lower deployment costs, as well as improved productivity as end users can be immediately productive – everything is right where they left it. Of course, you can also use a traditional wipe-and-load approach if you prefer, using the same tools that you use today with Windows 7.

Identity and Authentication

You can use Windows 10 and services like [Azure Active Directory](#) in new ways for cloud-based identity, authentication, and management. You can offer your users the ability to “**bring your own device**” (**BYOD**) or to “**choose your own device**” (**CYOD**) from a selection you make available. At the same time, you might be managing PCs and tablets that must be domain-joined because of specific applications or resources that are used on them.

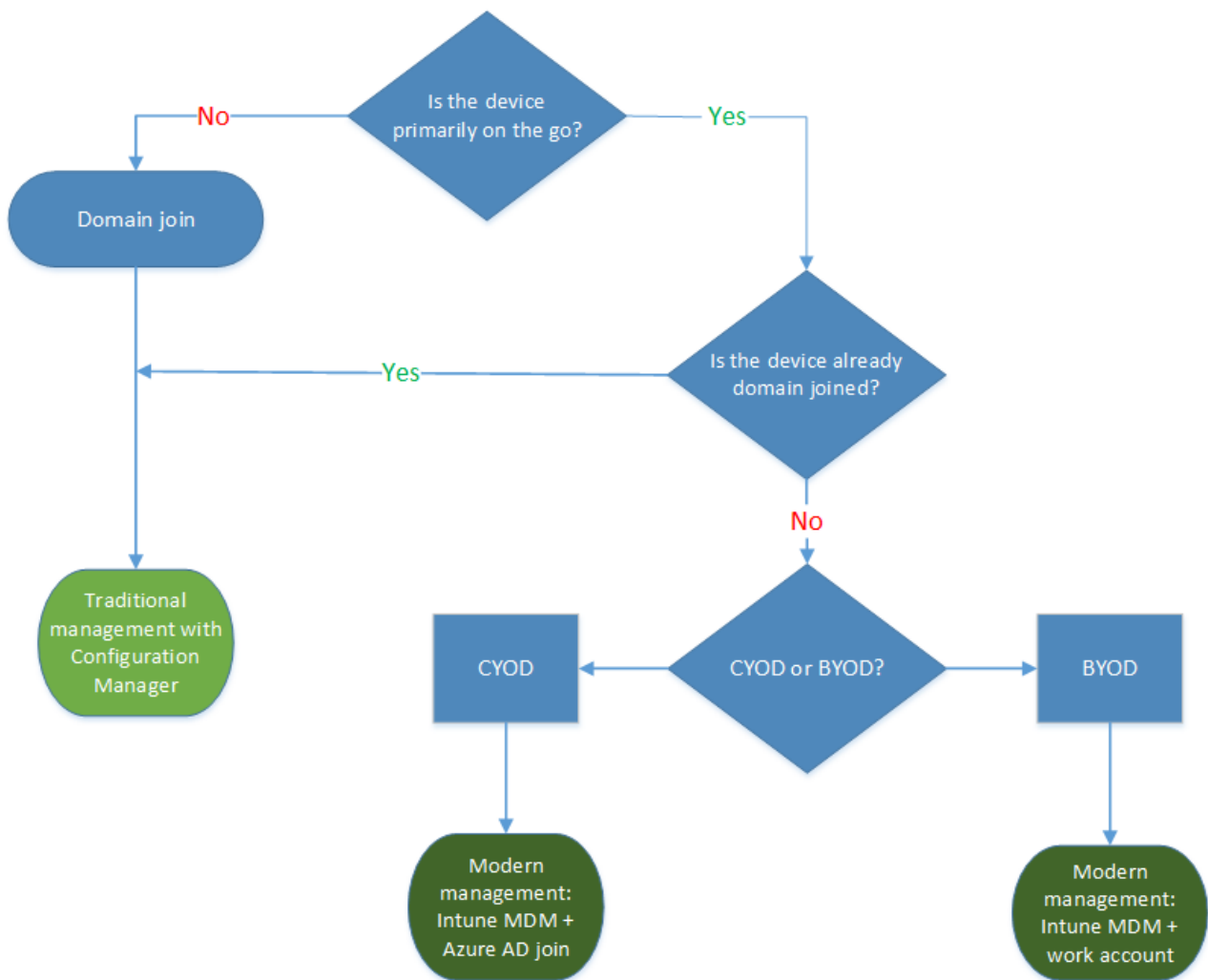
You can envision user and device management as falling into these two categories:

- **Corporate (CYOD) or personal (BYOD) devices used by mobile users for SaaS apps such as Office 365.** With Windows 10, your employees can self-provision their devices:
 - For corporate devices, they can set up corporate access with [Azure AD Join](#). When you offer them Azure AD Join with automatic Intune MDM enrollment, they can bring devices into a corporate-managed state in *one step*, all from the cloud. Azure AD Join is also a great solution for temporary staff, partners, or other part-time employees. These accounts can be kept separate from the on-premises AD domain but still access needed corporate resources.
 - Likewise, for personal devices, employees can use a new, simplified [BYOD experience](#) to add their work account to Windows, then access work resources on the device.
- **Domain joined PCs and tablets used for traditional applications and access to important resources.** These may be traditional applications and resources that require authentication or accessing highly sensitive or classified resources on-premises. With Windows 10, if you have an on-premises [Active Directory](#) domain that’s [integrated with Azure AD](#), when employee devices are joined, they automatically register with Azure AD. This provides:
 - Single sign-on to cloud and on-premises resources from everywhere
 - [Enterprise roaming of settings](#)
 - [Conditional access](#) to corporate resources based on the health or configuration of the device
 - [Windows Hello for Business](#)
 - Windows Hello

Domain joined PCs and tablets can continue to be managed with the [System Center Configuration Manager](#) client or Group Policy.

For more information about how Windows 10 and Azure AD optimize access to work resources across a mix of devices and scenarios, see [Using Windows 10 devices in your workplace](#).

As you review the roles in your organization, you can use the following generalized decision tree to begin to identify users or devices that require domain join. Consider switching the remaining users to Azure AD.



Settings and Configuration

Your configuration requirements are defined by multiple factors, including the level of management needed, the devices and data managed, and your industry requirements. Meanwhile, employees are frequently concerned about IT applying strict policies to their personal devices, but they still want access to corporate email and documents. With Windows 10, you can create a consistent set of configurations across PCs, tablets, and phones through the common MDM layer.

MDM: MDM gives you a way to configure settings that achieve your administrative intent without exposing every possible setting. (In contrast, Group Policy exposes fine-grained settings that you control individually.) One benefit of MDM is that it enables you to apply broader privacy, security, and application management settings through lighter and more efficient tools. MDM also allows you to target Internet-connected devices to manage policies without using GP that requires on-premises domain-joined devices. This makes MDM the best choice for devices that are constantly on the go.

Group Policy and System Center Configuration Manager: Your organization might still need to manage domain joined computers at a granular level such as Internet Explorer's 1,500 configurable Group Policy settings. If so, Group Policy and System Center Configuration Manager continue to be excellent management choices:

- Group Policy is the best way to granularly configure domain joined Windows PCs and tablets connected to the corporate network using Windows-based tools. Microsoft continues to add Group Policy settings with each new version of Windows.
- Configuration Manager remains the recommended solution for granular configuration with robust software deployment, Windows updates, and OS deployment.

Updating and Servicing

With Windows as a Service, your IT department no longer needs to perform complex imaging (wipe-and-load) processes with each new Windows release. Whether on current branch (CB) or current branch for business (CBB), devices receive the latest feature and quality updates through simple – often automatic – patching processes. For more information, see [Windows 10 deployment scenarios](#).

MDM with Intune provide tools for applying Windows updates to client computers in your organization. Configuration Manager allows rich management and tracking capabilities of these updates, including maintenance windows and automatic deployment rules.

Next steps

There are a variety of steps you can take to begin the process of modernizing device management in your organization:

Assess current management practices, and look for investments you might make today. Which of your current practices need to stay the same, and which can you change? Specifically, what elements of traditional management do you need to retain and where can you modernize? Whether you take steps to minimize custom imaging, re-evaluate settings management, or reassesses authentication and compliance, the benefits can be immediate. You can use the [MDM Migration Analysis Tool \(MMAT\)](#) to help determine which Group Policies are set for a target user/computer and cross-reference them against the list of available MDM policies.

Assess the different use cases and management needs in your environment. Are there groups of devices that could benefit from lighter, simplified management? BYOD devices, for example, are natural candidates for cloud-based management. Users or devices handling more highly regulated data might require an on-premises Active Directory domain for authentication. Configuration Manager and EMS provide you the flexibility to stage implementation of modern management scenarios while targeting different devices the way that best suits your business needs.

Review the decision trees in this article. With the different options in Windows 10, plus Configuration Manager and Enterprise Mobility + Security, you have the flexibility to handle imaging, authentication, settings, and management tools for any scenario.

Take incremental steps. Moving towards modern device management doesn't have to be an overnight transformation. New operating systems and devices can be brought in while older ones remain. With this "managed diversity," users can benefit from productivity enhancements on new Windows 10 devices, while you continue to maintain older devices according to your standards for security and manageability. Starting with Windows 10, version 1803, the new policy [MDMWinsOverGP](#) was added to allow MDM policies to take precedence over GP when both GP and its equivalent MDM policies are set on the device. You can start implementing MDM policies while keeping your GP environment. Here is the list of MDM policies with equivalent GP - [Policies supported by GP](#)

Optimize your existing investments. On the road from traditional on-premises management to modern cloud-based management, take advantage of the flexible, hybrid architecture of Configuration Manager and Intune. Starting with Configuration Manager 1710, co-management enables you to concurrently manage Windows 10 devices by using both Configuration Manager and Intune. See these topics for details:

- [Co-management for Windows 10 devices](#)
- [Prepare Windows 10 devices for co-management](#)
- [Switch Configuration Manager workloads to Intune](#)
- [Co-management dashboard in System Center Configuration Manager](#)

Related topics

- [What is Intune?](#)
- [Windows 10 Policy CSP](#)
- [Windows 10 Configuration service Providers](#)

Windows 10 Mobile deployment and management guide

6/6/2019 • 71 minutes to read • [Edit Online](#)

Applies to:

- Windows 10 Mobile, version 1511 and Windows 10 Mobile, version 1607

This guide helps IT professionals plan for and deploy Windows 10 Mobile devices.

Employees increasingly depend on smartphones to complete daily work tasks, but these devices introduce unique management and security challenges. Whether providing corporate devices or allowing people to use their personal devices, IT needs to deploy and manage mobile devices and apps quickly to meet business goals. However, they also need to ensure that the apps and data on those mobile devices are protected against cybercrime or loss. Windows 10 Mobile helps organizations directly address these challenges with robust, flexible, built-in mobile device and app management technologies. Windows 10 supports end-to-end device lifecycle management to give companies control over their devices, data, and apps. Devices can easily be incorporated into standard lifecycle practices, from device enrollment, configuration, and application management to maintenance, monitoring, and retirement using a comprehensive mobile device management solution.

In this article

- [Deploy](#)
- [Configure](#)
- [Apps](#)
- [Manage](#)
- [Retire](#)

Deploy

Windows 10 Mobile has a built-in device management client to deploy, configure, maintain, and support smartphones. Common to all editions of the Windows 10 operating system, including desktop, mobile, and Internet of Things (IoT), this client provides a single interface through which Mobile Device Management (MDM) solutions can manage any device that runs Windows 10. Because the MDM client integrates with identity management, the effort required to manage devices throughout the lifecycle is greatly reduced. Windows 10 includes comprehensive MDM capabilities that can be managed by Microsoft management solutions, such as Microsoft Intune or System Center Configuration Manager, as well as many third-party MDM solutions. There is no need to install an additional, custom MDM app to enroll devices and bring them under MDM control. All MDM system vendors have equal access to Windows 10 Mobile device management application programming interfaces (APIs), giving IT organizations the freedom to select whichever system best fits their management requirements, whether Microsoft Intune or a third-party MDM product. For more information about Windows 10 Mobile device management APIs, see [Mobile device management](#).

Deployment scenarios

Applies to: Corporate and personal devices

The built-in MDM client is common to all editions of the Windows 10 operating system, including desktop, mobile, and Internet of Things (IoT). The client provides a single interface through which you can manage any device that runs Windows 10. The client has two important roles: device enrollment in an MDM system and device management.

Organizations typically have two scenarios to consider when it comes to device deployment: Bring Your Own (BYO) personal devices and Choose Your Own (CYO) company-owned devices. In both cases, the device must be enrolled in an MDM system, which would configure it with settings appropriate for the organization and the employee. Windows 10 Mobile device management capabilities support both personal devices used in the BYO scenario and corporate devices used in the CYO scenario. The operating system offers a flexible approach to registering devices with directory services and MDM systems. IT organizations can provision comprehensive device-configuration profiles based on their business needs to control and protect mobile business data. Apps can be provisioned easily to personal or corporate devices through the Microsoft Store for Business, or by using their MDM system, which can also work with the Microsoft Store for Business for public store apps. Knowing who owns the device and what the employee will use it for are the major factors in determining your management strategy and which controls your organization should put in place. Whether personal devices, corporate devices, or a mixture of the two, deployment processes and configuration policies may differ.

For **personal devices**, companies need to be able to manage corporate apps and data on the device without impeding the employee’s ability to personalize it to meet their individual needs. The employee owns the device and corporate policy allows them to use it for both business and personal purposes, with the ability to add personal apps at their discretion. The main concern with personal devices is how organizations can prevent corporate data from being compromised, while still keeping personal data private and under the sole control of the employee. This requires that the device be able to support separation of apps and data with strict control of business and personal data traffic.

For **corporate devices**, organizations have a lot more control. IT can provide a selected list of supported device models to employees, or they can directly purchase and preconfigure them. Because devices are owned by the company, employees can be limited as to how much they can personalize these devices. Security and privacy concerns may be easier to navigate, because the device falls entirely under existing company policy.

Device enrollment

Applies to: Corporate and personal devices

The way in which personal and corporate devices are enrolled into an MDM system differs. Your operations team should consider these differences when determining which approach is best for mobile workers in your organization.

Device initialization and enrollment considerations

	Personal devices	Corporate devices
Ownership	Employee	Organization
Device Initialization In the Out-of-the-Box Experience (OOBE), the first time the employee starts the device, they are requested to add a cloud identity to the device.	The primary identity on the device is a personal identity. Personal devices are initiated with a Microsoft Account (MSA), which uses a personal email address.	The primary identity on the device is an organizational identity. Corporate devices are initialized with an organizational account (account@corporatedomain.ext). Initialization of a device with a corporate account is unique to Windows 10. No other mobile platform currently offers this capability. The default option is to use an Azure Active Directory organizational identity. Skipping the account setup in OOBE will result in the creation of a local account. The only option to add a cloud account later is to add an MSA, putting this device into a personal device deployment scenario. To start over, the device will have to be reset.

<p>Device Enrollment</p> <p>Enrolling devices in an MDM system helps control and protect corporate data while keeping workers productive.</p>	<p>Device enrollment can be initiated by employees. They can add an Azure account as a secondary account to the Windows 10 Mobile device. Provided the MDM system is registered with your Azure AD, the device is automatically enrolled in the MDM system when the user adds an Azure AD account as a secondary account (MSA+AAD+MDM). If your organization does not have Azure AD, the employee's device will automatically be enrolled into your organization's MDM system (MSA+MDM). MDM enrollment can also be initiated with a provisioning package. This option enables IT to offer easy-to-use self-service enrollment of personal devices. Provisioning is currently only supported for MDM-only enrollment (MSA+MDM).</p>	<p>The user initiates MDM enrollment by joining the device to the Azure AD instance of their organization. The device is automatically enrolled in the MDM system when the device registers in Azure AD. This requires your MDM system to be registered with your Azure AD (AAD+MDM).</p>
--	---	---

Recommendation: Microsoft recommends Azure AD registration and automatic MDM enrollment for corporate devices (AAD+MDM) and personal devices (MSA+AAD+MDM). This requires Azure AD Premium.

Identity management

Applies to: Corporate and personal devices

Employees can use only one account to initialize a device so it's imperative that your organization controls which account is enabled first. The account chosen will determine who controls the device and influence your management capabilities.

Note: Why must the user add an account to the device in OOB? Windows 10 Mobile are single user devices and the user accounts give access to a number of default cloud services that enhance the productivity and entertainment value of the phone for the user. Such services are: Store for downloading apps, Groove for music and entertainment, Xbox for gaming, etc. Both an [MSA](#) and an [Azure AD account](#) give access to these services.

The following table describes the impact of identity choice on device management characteristics of the personal and corporate device scenarios.

Identity choice considerations for device management

	Personal identity	Work identity
First account on the device	Microsoft Account	Azure AD account
Ease of enrollment	Employees use their Microsoft Account to activate the device. Then, they use their Azure AD account (organizational identity) to register the device in Azure AD and enroll it with the company's MDM solution (MSA+AAD+MDM).	Employees use their Azure AD account to register the device in Azure AD and automatically enroll it with the organization's MDM solution (AAD+MDM – requires Azure AD Premium).

Credential management	Employees sign in to the device with Microsoft Account credentials. Users cannot sign in to devices with Azure AD credentials, even if they add the credentials after initial activation with a Microsoft account.	Employees sign in to the device with Azure AD credentials. IT can block the addition of a personal identity, such as an MSA or Google Account. IT controls all devices access policies, without limitations.
Ability to block the use of a personal identity on the device	No	Yes
User settings and data roaming across multiple Windows devices	User and app settings roam across all devices activated with the same personal identity through OneDrive.	If the device is activated with an MSA, then adds an Azure AD account, user app settings roam. If you add your MSA to an Azure AD-joined device, this will not be the case. Microsoft is investigating Enterprise roaming for a future release.
Level of control	Organizations can apply most of the available restrictive policies to devices and disable the Microsoft account. You can prevent users from reclaiming full control over their devices by unenrolling them from the organization's MDM solution or resetting the device. Legal limitations may apply. For more information, contact your legal department.	Organizations are free to apply any restrictive policies to devices to bring them in line with corporate standards and compliance regulations. They can also prevent the user from unenrolling the device from the enterprise.
Information Protection	You can apply policies to help protect and contain corporate apps and data on the devices and prevent intellectual property leaks, but still provide employees with full control over personal activities like downloading and installing apps and games.	Companies can block personal use of devices. Using organizational identities to initialize devices gives organizations complete control over devices and allows them to prevent personalization.
App purchases	Employees can purchase and install apps from the Store using a personal credit card.	Employees can install apps from your Store for Business. Employees cannot install or purchase app from the Store without the addition of an MSA.

Note: In the context of [Windows-as-a-Service](#), differentiation of MDM capabilities will change in the future.

Infrastructure choices

Applies to: Corporate and personal devices

For both personal and corporate deployment scenarios, an MDM system is the essential infrastructure required to deploy and manage Windows 10 Mobile devices. An Azure AD premium subscription is recommended as an identity provider and required to support certain capabilities. Windows 10 Mobile allows you to have a pure cloud-based infrastructure or a hybrid infrastructure that combines Azure AD identity management with an on-premises management system to manage devices. Microsoft now also supports a pure on-premises solution to manage Windows 10 Mobile devices with [Configuration Manager](#).

Azure Active Directory Azure AD is a cloud-based directory service that provides identity and access management. You can integrate it with existing on-premises directories to create a hybrid identity solution. Organizations that use Microsoft Office 365 or Intune are already using Azure AD, which has three editions: Free Basic, and Premium (see [Azure Active Directory editions](#)). All editions support Azure AD device registration, but

the Premium edition is required to enable MDM auto-enrollment and conditional access based on device state.

Mobile Device Management Microsoft [Intune](#), part of the Enterprise Mobility + Security, is a cloud-based MDM system that manages devices off premises. Like Office 365, Intune uses Azure AD for identity management so employees use the same credentials to enroll devices in Intune that they use to sign into Office 365. Intune supports devices that run other operating systems, such as iOS and Android, to provide a complete MDM solution. You can also integrate Intune with Configuration Manager to gain a single console for managing all devices in the cloud and on premises, mobile or PC. For more information, see [Manage Mobile Devices with Configuration Manager and Microsoft Intune](#). For guidance on choosing between a stand-alone Intune installation and Intune integrated with System Center Configuration Manager, see [Choose between Intune by itself or integrating Intune with System Center Configuration Manager](#). Multiple MDM systems support Windows 10 and most support personal and corporate device deployment scenarios. MDM providers that support Windows 10 Mobile currently include: AirWatch, Citrix, MobileIron, SOTI, Blackberry and others. Most industry-leading MDM vendors already support integration with Azure AD. You can find the MDM vendors that support Azure AD in [Azure Marketplace](#). If your organization doesn't use Azure AD, the user must use an MSA during OOB before enrolling the device in your MDM using a corporate account.

Note: Although not covered in this guide, you can use Exchange ActiveSync (EAS) to manage mobile devices instead of using a full-featured MDM system. EAS is available in Microsoft Exchange Server 2010 or later and Office 365. In addition, Microsoft recently added MDM capabilities powered by Intune to Office 365. MDM for Office 365 supports mobile devices only, such as those running Windows 10 Mobile, iOS, and Android. MDM for Office 365 offers a subset of the management capabilities found in Intune, including the ability to remotely wipe a device, block a device from accessing Exchange Server email, and configure device policies (e.g., passcode requirements). For more information about MDM for Office 365 capabilities, see [Overview of Mobile Device Management for Office 365](#).

Cloud services On mobile devices that run Windows 10 Mobile, users can easily connect to cloud services that provide user notifications and collect diagnostic and usage data. Windows 10 Mobile enables organizations to manage how devices consume these cloud services.

Windows Push Notification Services The Windows Push Notification Services enable software developers to send toast, tile, badge, and raw updates from their cloud services. It provides a mechanism to deliver updates to users in a power-efficient and dependable way. However, push notifications can affect battery life so the battery saver in Windows 10 Mobile limits background activity on the devices to extend battery life. Users can configure battery saver to turn on automatically when the battery drops below a set threshold. Windows 10 Mobile disables the receipt of push notifications to save energy when battery saver is on. However, there is an exception to this behavior. In Windows 10 Mobile, the Always allowed battery saver setting (found in the Settings app) allows apps to receive push notifications even when battery saver is on. Users can manually configure this list, or IT can use the MDM system to configure the battery saver settings URI scheme in Windows 10 Mobile (ms-settings:batterysaver-settings).

For more information about health attestation in Windows 10 Mobile, see the [Windows 10 Mobile security guide](#).

Windows Update for Business Microsoft designed Windows Update for Business to provide IT administrators with additional Windows Update-centric management capabilities, such as the ability to deploy updates to groups of devices and to define maintenance windows for installing updates.

Microsoft Store for Business The Microsoft Store for Business is the place where IT administrators can find, acquire, manage, and distribute apps to Windows 10 devices. This includes both internal line-of-business (LOB) apps, as well as commercially available third-party apps.

Configure

MDM administrators can define and implement policy settings on any personal or corporate device enrolled in an

MDM system. What configuration settings you use will differ based on the deployment scenario, and corporate devices will offer IT the broadest range of control.

Note: This guide helps IT professionals understand management options available for the Windows 10 Mobile OS. Please consult your MDM system documentation to understand how these policies are enabled by your MDM vendor. Not all MDM systems support every setting described in this guide. Some support custom policies through OMA-URI XML files. See [Microsoft Intune support for Custom Policies](#). Naming conventions may also vary among MDM vendors.

Account profile

Applies to: Corporate devices

Enforcing what accounts employees can use on a corporate device is important for avoiding data leaks and protecting privacy. Limiting the device to just one account controlled by the organization will reduce the risk of a data breach. However, you can choose to allow employees to add a personal Microsoft Account or other consumer email accounts.

- **Allow Microsoft Account** Specifies whether users are allowed to add a Microsoft Account to the device and use this account to authenticate to cloud services, such as purchasing apps in Microsoft Store, Xbox, or Groove.
- **Allow Adding Non-Microsoft Accounts** Specifies whether users are allowed to add email accounts other than Microsoft accounts.

Email accounts

Applies to: Corporate and personal devices

Email and associated calendar and contacts are the primary apps that users access on their smartphones. Configuring them properly is key to the success of any mobility program. In both corporate and personal device deployment scenarios, these email account settings get deployed immediately after enrollment. Using your corporate MDM system, you can define corporate email account profiles, deploy them to devices, and manage inbox policies.

- Most corporate email systems leverage **Exchange ActiveSync (EAS)**. For more details on configuring EAS email profiles, see the [ActiveSync CSP](#).
- **Simple Mail Transfer Protocol (SMTP)** email accounts can also be configured with your MDM system. For more detailed information on SMTP email profile configuration, see the [Email CSP](#). Microsoft Intune does not currently support the creation of an SMTP email profile.

Device Lock restrictions

Applies to: Corporate and personal devices

It's common practice to protect a device that contains corporate information with a passcode when it is not in use. As a best practice, Microsoft recommends that you implement a device lock policy for Windows 10 Mobile devices for securing apps and data. You can use a complex password or numeric PIN to lock devices. Introduced with Windows 10, [Windows Hello](#) allows you to use a PIN, a companion device (like Microsoft band), or biometrics to validate your identity to unlock Windows 10 Mobile devices.

Note: When Windows 10 first shipped, it included Microsoft Passport and Windows Hello, which worked together to provide multifactor authentication. To simplify deployment and improve supportability, Microsoft has combined these technologies into a single solution under the Windows Hello name. Customers who have already deployed these technologies will not experience any change in functionality. Customers who have yet to evaluate Windows Hello will find it easier to deploy due to simplified policies, documentation, and semantics. To use Windows Hello with biometrics, specialized hardware, including fingerprint reader, illuminated IR sensor, or other biometric sensors is required. Hardware based protection of the Windows Hello credentials requires TPM 1.2 or greater; if no TPM exists or is configured, credentials/keys protection will be software-based. Companion devices must be paired with Windows 10 PC's via Bluetooth. To use a Windows

Hello companion device that enables the user to roam with their Windows Hello credentials requires Pro or Enterprise edition on the Windows 10 PC being signed into.

Most of the device lock restriction policies have been available via ActiveSync and MDM since Windows Phone 7 and are still available today for Windows 10 Mobile. If you are deploying Windows 10 devices in a personal device deployment scenario, these settings would apply.

- **Device Password Enabled** Specifies whether users are required to use a device lock password.
- **Allow Simple Device Password** Whether users can use a simple password (e.g., 1111 or 1234).
- **Alphanumeric Device Password Required** Whether users need to use an alphanumeric password. When configured, Windows prompts the user with a full device keyboard to enter a complex password. When not configured, the user will be able to enter a numeric PIN on the keyboard.
- **Min Device Password Complex Characters** The number of password element types (i.e., uppercase letters, lowercase letters, numbers, or punctuation) required to create strong passwords.
- **Device Password History** The number of passwords Windows 10 Mobile remembers in the password history (Users cannot reuse passwords in the history to create new passwords.)
- **Min Device Password Length** The minimum number of characters required to create new passwords.
- **Max Inactivity Time Device Lock** The number of minutes of inactivity before devices are locked and require a password to unlock.
- **Allow Idle Return Without Password** Whether users are required to re-authenticate when their devices return from a sleep state before the inactivity time was reached.
- **Max Device Password Failed Attempts** The number of authentication failures allowed before a device is wiped (A value of zero disables device wipe functionality.)
- **Screen Timeout While Locked** The number of minutes before the lock screen times out (this policy influences device power management).
- **Allow Screen Timeout While Locked User Configuration** Whether users can manually configure screen timeout while the device is on the lock screen (Windows 10 Mobile ignores the **Screen Timeout While Locked** setting if you disable this setting).

Settings related to Windows Hello would be important device lock settings to configure if you are deploying devices using the corporate deployment scenario. Microsoft made it a requirement for all users to create a numeric passcode as part of Azure AD Join. This policy default requires users to select a four-digit passcode, but this can be configured with an AAD-registered MDM system to whatever passcode complexity your organization desires. If you are using Azure AD with an automatic MDM enrollment mechanism, these policy settings are automatically applied during device enrollment.

You will notice that some of the settings are very similar, specifically those related to passcode length, history, expiration, and complexity. If you set the policy in multiple places, both policies will be applied, with the strongest policy retained. Read [PassportForWork CSP](#), [DeviceLock CSP](#) (Windows Phone 8.1), and [Policy CSP](#) for more detailed information.

Prevent changing of settings

Applies to: Corporate devices

Employees are usually allowed to change certain personal device settings that you may want to lock down on corporate devices. Employees can interactively adjust certain settings of the phone through the settings applets. Using MDM, you can limit what users are allowed to change.

- **Allow Your Account** Specifies whether users are able to change account configuration in the Your Email and Accounts panel in Settings
- **Allow VPN** Allows the user to change VPN settings
- **Allow Data Sense** Allows the user to change Data Sense settings

- **Allow Date Time** Allows the user to change data and time setting
- **Allow Edit Device Name** Allows users to change the device name
- **Allow Speech Model Update** Specifies whether the device will receive updates to the speech recognition and speech synthesis models (to improve accuracy and performance)

Hardware restrictions

Applies to: Corporate devices

Windows 10 Mobile devices use state-of-the-art technology that includes popular hardware features such as cameras, global positioning system (GPS) sensors, microphones, speakers, near-field communication (NFC) radios, storage card slots, USB interfaces, Bluetooth interfaces, cellular radios, and Wi Fi. You can use hardware restrictions to control the availability of these features.

The following lists the MDM settings that Windows 10 Mobile supports to configure hardware restrictions.

Note: Some of these hardware restrictions provide connectivity and assist in data protection.

- **Allow NFC:** Whether the NFC radio is enabled
- **Allow USB Connection:** Whether the USB connection is enabled (doesn't affect USB charging)
- **Allow Bluetooth:** Whether users can enable and use the Bluetooth radio on their devices
- **Allow Bluetooth Advertising:** Whether the device can act as a source for Bluetooth advertisements and be discoverable to other devices
- **Allow Bluetooth Discoverable Mode:** Whether the device can discover other devices (e.g., headsets)
- **Allow Bluetooth pre-pairing** Whether to allow specific bundled Bluetooth peripherals to automatically pair with the host device
- **Bluetooth Services Allowed List:** The list of Bluetooth services and profiles to which the device can connect
- **Set Bluetooth Local Device Name:** The local Bluetooth device name
- **Allow Camera:** Whether the camera is enabled
- **Allow Storage Card:** Whether the storage card slot is enabled
- **Allow Voice Recording:** Whether the user can use the microphone to create voice recordings
- **Allow Location:** Whether the device can use the GPS sensor or other methods to determine location so applications can use location information

Certificates

Applies to: Personal and corporate devices

Certificates help improve security by providing account authentication, Wi Fi authentication, VPN encryption, and SSL encryption of web content. Although users can manage certificates on devices manually, it's a best practice to use your MDM system to manage those certificates throughout their entire lifecycle – from enrollment through renewal and revocation. To install certificates manually, you can post them on Microsoft Edge website or send them directly via email, which is ideal for testing purposes. Using SCEP and MDM systems, certificate management is completely transparent and requires no user intervention, helping improve user productivity, and reduce support calls. Your MDM system can automatically deploy these certificates to the devices' certificate stores after you enroll the device (as long as the MDM system supports the Simple Certificate Enrollment Protocol (SCEP) or Personal Information Exchange (PFX)). The MDM server can also query and delete SCEP enrolled client certificate (including user installed certificates), or trigger a new enrollment request before the current certificate is expired. In addition to SCEP certificate management, Windows 10 Mobile supports deployment of PFX certificates. The table below lists the Windows 10 Mobile PFX certificate deployment settings. Get more detailed information about MDM certificate management in the [Client Certificate Install CSP](#) and [Install digital certificates on Windows 10 Mobile](#). Use the Allow Manual Root Certificate Installation setting to prevent users from manually installing root and intermediate CA certificates intentionally or accidentally.

Note: To diagnose certificate-related issues on Windows 10 Mobile devices, use the free Certificates app in Microsoft Store. This Windows 10 Mobile app can help you:

- View a summary of all personal certificates
- View the details of individual certificates
- View the certificates used for VPN, Wi-Fi, and email authentication
- Identify which certificates may have expired
- Verify the certificate path and confirm that you have the correct intermediate and root CA certificates
- View the certificate keys stored in the device TPM

Wi-Fi profiles

Applies to: Corporate and personal devices

Wi-Fi is used on mobile devices as much as, or more than, cellular data connections. Most corporate Wi-Fi networks require certificates and other complex information to restrict and secure user access. This advanced Wi-Fi information is difficult for typical users to configure, but MDM systems can fully configure these Wi-Fi profiles without user intervention. You can create multiple Wi-Fi profiles in your MDM system. The below table lists the Windows 10 Mobile Wi-Fi connection profile settings that can be configured by administrators.

- **SSID** The case-sensitive name of the Wi-Fi network Service Set Identifier
- **Security type** The type of security the Wi-Fi network uses; can be one of the following authentication types:
 - Open 802.11
 - Shared 802.11
 - WPA-Enterprise 802.11
 - WPA-Personal 802.11
 - WPA2-Enterprise 802.11
 - WPA2-Personal 802.11
- **Authentication encryption** The type of encryption the authentication uses; can be one of the following encryption methods:
 - None (no encryption)
 - Wired Equivalent Privacy
 - Temporal Key Integrity Protocol
 - Advanced Encryption Standard (AES)
- **Extensible Authentication Protocol Transport Layer Security (EAP-TLS)** WPA-Enterprise 802.11 and WPA2-Enterprise 802.11 security types can use EAP-TLS with certificates for authentication
- **Protected Extensible Authentication Protocol with Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2)** WPA-Enterprise 802.11 and WPA2-Enterprise 802.11 security types can use PEAP-MSCHAPv2 with a user name and password for authentication
- **Shared key** WPA-Personal 802.11 and WPA2-Personal 802.11 security types can use a shared key for authentication.
- **Proxy** The configuration of any network proxy that the Wi-Fi connection requires (to specify the proxy server, use its fully qualified domain name [FQDN], Internet Protocol version 4 [IPv4] address, IP version 6 [IPv6] address, or IPvFuture address)
- **Disable Internet connectivity checks** Whether the Wi-Fi connection should check for Internet connectivity
- **Proxy auto-configuration URL** A URL that specifies the proxy auto-configuration file
- **Enable Web Proxy Auto-Discovery Protocol (WPAD)** Specifies whether WPAD is enabled

In addition, you can set a few device wide Wi-Fi settings.

- **Allow Auto Connect to Wi-Fi Sense Hotspots** Whether the device will automatically detect and connect to Wi-Fi networks

- **Allow Manual Wi-Fi Configuration** Whether the user can manually configure Wi-Fi settings
- **Allow Wi-Fi** Whether the Wi-Fi hardware is enabled
- **Allow Internet Sharing** Allow or disallow Internet sharing
- **WLAN Scan Mode** How actively the device scans for Wi-Fi networks

Get more detailed information about Wi-Fi connection profile settings in the [Wi-Fi CSP](#) and [Policy CSP](#).

APN profiles

Applies to: Corporate devices

An Access Point Name (APN) defines network paths for cellular data connectivity. Typically, you define just one APN for a device in collaboration with a mobile operator, but you can define multiple APNs if your company uses multiple mobile operators. An APN provides a private connection to the corporate network that is unavailable to other companies on the mobile operator network. You can define and deploy APN profiles in MDM systems that configure cellular data connectivity for Windows 10 Mobile. Devices running Windows 10 Mobile can have only one APN profile. The following lists the MDM settings that Windows 10 Mobile supports for APN profiles.

- **APN name** The APN name
- **IP connection type** The IP connection type; set to one of the following values:
 - IPv4 only
 - IPv6 only
 - IPv4 and IPv6 concurrently
 - IPv6 with IPv4 provided by 4Gxlat
- **LTE attached** Whether the APN should be attached as part of an LTE Attach
- **APN class ID** The globally unique identifier that defines the APN class to the modem
- **APN authentication type** The APN authentication type; set to one of the following values:
 - None
 - Auto
 - PAP
 - CHAP
 - MSCHAPv2
- **User name** The user account when users select Password Authentication Protocol (PAP), CHAP, or MSCHAPv2 authentication in APN authentication type
- **Password** The password for the user account specified in User name
- **Integrated circuit card ID** The integrated circuit card ID associated with the cellular connection profile
- **Always on** Whether the connection manager will automatically attempt to connect to the APN whenever it is available
- **Connection enabled** Specifies whether the APN connection is enabled
- **Allow user control** Allows users to connect with other APNs than the enterprise APN
- **Hide view** Whether the cellular UX will allow the user to view enterprise APNs

Get more detailed information about APN settings in the [APN CSP](#).

Proxy

Applies to: Corporate devices

The below lists the Windows 10 Mobile settings for managing APN proxy settings for Windows 10 Mobile device connectivity.

- **Connection name** Specifies the name of the connection the proxy is associated with (this is the APN name of a configured connection)
- **Bypass Local** Specifies if the proxy should be bypassed when local hosts are accessed by the device

- **Enable** Specifies if the proxy is enabled
- **Exception** Specifies a semi-colon delimited list of external hosts which should bypass the proxy when accessed
- **User Name** Specifies the username used to connect to the proxy
- **Password** Specifies the password used to connect to the proxy
- **Server** Specifies the name of the proxy server
- **Proxy connection type** The proxy connection type, supporting: Null proxy, HTTP, WAP, SOCKS4
- **Port** The port number of the proxy connection

For more details on proxy settings, see [CM_ProxyEntries CSP](#).

VPN

Applies to: Corporate and personal devices

Organizations often use a VPN to control access to apps and resources on their company's intranet. In addition to native Microsoft Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Internet Key Exchange Protocol version 2 (IKEv2) VPNs, Windows 10 Mobile supports SSL VPN connections, which require a downloadable plugin from the Microsoft Store and are specific to the VPN vendor of your choice. These plugins work like apps and can be installed directly from the Microsoft Store using your MDM system (see App Management).

You can create and provision multiple VPN connection profiles and then deploy them to managed devices that run Windows 10 Mobile. To create a VPN profile that uses native Windows 10 Mobile VPN protocols (such as IKEv2, PPTP, or L2TP), you can use the following settings:

- **VPN Servers** The VPN server for the VPN profile
- **Routing policy type** The type of routing policy the VPN profile uses can be set to one of the following values:
 - Split tunnel. Only network traffic destined to the intranet goes through the VPN connection
 - Force tunnel. All traffic goes through the VPN connection
- **Tunneling protocol type** The tunneling protocol used for VPN profiles that use native Windows 10 Mobile VPN protocols can be one of the following values: PPTP, L2TP, IKEv2, Automatic
- **User authentication method** The user authentication method for the VPN connection can have a value of EAP or MSChapv2 (Windows 10 Mobile does not support the value MSChapv2 for IKEv2-based VPN connections)
- **Machine certificate** The machine certificate used for IKEv2-based VPN connections
- **EAP configuration** To create a single sign-on experience for VPN users using certificate authentication, you need to create an Extensible Authentication Protocol (EAP) configuration XML file and include it in the VPN profile
- **L2tpPsk** The pre-shared key used for an L2TP connection
- **Cryptography Suite** Enable the selection of cryptographic suite attributes used for IPsec tunneling

Note: The easiest way to create a profile for a single sign-on experience with an EAP configuration XML is through the rasphone tool on a Windows 10 PC. Once you run the rasphone.exe, the configuration wizard will walk you through the necessary steps. For step-by-step instructions on creating the EAP configuration XML blob, see EAP configuration. You can use the resulting XML blob in the MDM system to create the VPN profile on Windows 10 Mobile phone. If you have multiple certificates on the devices, you may want to configure filtering conditions for automatic certificate selection, so the employee does not need to select an authentication certificate every time the VPN is turned on. See this article for details. Windows 10 for PCs and Windows 10 Mobile have the same VPN client.

Microsoft Store-based VPN plugins for the VPN connection allow you to create a VPN plugin profile with the following attributes:

- **VPN server** A comma-separated list of VPN servers; you can specify the servers with a URL, fully qualified host name, or IP address
- **Custom configuration** An HTML-encoded XML blob for SSL-VPN plugin-specific configuration information (e.g., authentication information) that the plugin provider requires
- **Microsoft Store VPN plugin family name** Specifies the Microsoft Store package family name for the Microsoft Store-based VPN plugin

In addition, you can specify per VPN Profile:

- **App Trigger List** You can add an App Trigger List to every VPN profile. The app specified in the list will automatically trigger the VPN profile for intranet connectivity. When multiple VPN profiles are needed to serve multiple apps, the operating system automatically establishes the VPN connection when the user switches between apps. Only one VPN connection at a time can be active. In the event the device drops the VPN connection, Windows 10 Mobile automatically reconnects to the VPN without user intervention.
- **Route List** List of routes to be added to the routing table for the VPN interface. This is required for split tunneling cases where the VPN server site has more subnets than the default subnet based on the IP assigned to the interface.
- **Domain Name Information List** Name Resolution Policy Table (NRPT) rules for the VPN profile.
- **Traffic Filter List** Specifies a list of rules. Only traffic that matches these rules can be sent via the VPN Interface.
- **DNS suffixes** A comma-separated list of DNS suffixes for the VPN connection. Any DNS suffixes in this list are automatically added to Suffix Search List.
- **Proxy** Any post-connection proxy support required for the VPN connection; including Proxy server name and Automatic proxy configuration URL. Specifies the URL for automatically retrieving proxy server settings.
- **Always on connection** Windows 10 Mobile features always-on VPN, which makes it possible to automatically start a VPN connection when a user signs in. The VPN stays connected until the user manually disconnects it.
- **Remember credentials** Whether the VPN connection caches credentials.
- **Trusted network detection** A comma-separated list of trusted networks that causes the VPN not to connect when the intranet is directly accessible (Wi-Fi).
- **Enterprise Data Protection Mode ID** Enterprise ID, which is an optional field that allows the VPN to automatically trigger based on an app defined with a Windows Information Protection policy.
- **Device Compliance** To set up Azure AD-based Conditional Access for VPN and allow that SSO with a certificate different from the VPN Authentication certificate for Kerberos Authentication in the case of Device Compliance.
- **Lock Down VPN profile** A Lock Down VPN profile has the following characteristics:
 - It is an always-on VPN profile.
 - It can never be disconnected.
 - If the VPN profile is not connected, the user has no network connectivity.
 - No other VPN profiles can be connected or modified.
- **ProfileXML** In case your MDM system does not support all the VPN settings you want to configure, you can create an XML file that defines the VPN profile you want to apply to all the fields you require.

For more details about VPN profiles, see the [VPNv2 CSP](#)

Some device-wide settings for managing VPN connections can help you manage VPNs over cellular data connections, which in turn helps reduce costs associated with roaming or data plan charges.

- **Allow VPN** Whether users can change VPN settings
- **Allow VPN Over Cellular** Whether users can establish VPN connections over cellular networks
- **Allow VPN Over Cellular when Roaming** Whether users can establish VPN connections over cellular networks when roaming

Storage management

Applies to: Corporate and personal devices

Protecting the apps and data stored on a device is critical to device security. One method for helping protect your apps and data is to encrypt internal device storage. The [device encryption](#) in Windows 10 Mobile helps protect corporate data against unauthorized access, even when an unauthorized user has physical possession of the device.

Windows 10 Mobile also has the ability to install apps on a secure digital (SD) card. The operating system stores apps on a partition specifically designated for that purpose. This feature is always on so you don't need to set a policy explicitly to enable it.

The SD card is uniquely paired with a device. No other devices can see the apps or data on the encrypted partition, but they can access the data stored on the unencrypted partition of the SD card, such as music or photos. This gives users the flexibility to use an SD card while still protecting the confidential apps and data on it.

You can disable the **Allow Storage Card** setting if you wish to prevent users from using SD cards entirely. If you choose not to encrypt storage, you can help protect your corporate apps and data by using the Restrict app data to the system volume and Restrict apps to the system volume settings. These help ensure that users cannot copy your apps and data to SD cards.

Here is a list of MDM storage management settings that Windows 10 Mobile provides.

- **Allow Storage Card** Whether the use of storage cards for data storage is allowed
- **Require Device Encryption** Whether internal storage is encrypted (when a device is encrypted, you cannot use a policy to turn encryption off)
- **Encryption method** Specifies the BitLocker drive encryption method and cipher strength; can be one of the following values:
 - AES-Cipher Block Chaining (CBC) 128-bit
 - AES-CBC 256-bit
 - XEX-based tweaked-codebook mode with cipher text stealing (XTS)–AES (XTS-AES) 128-bit (this is the default)
 - XTS-AES-256-bit
- **Allow Federal Information Processing Standard (FIPS) algorithm policy** Whether the device allows or disallows the FIPS algorithm policy
- **SSL cipher suites** Specifies a list of the allowed cryptographic cipher algorithms for SSL connections
- **Restrict app data to the system volume** Specifies whether app data is restricted to the system drive
- **Restrict apps to the system volume** Specifies whether apps are restricted to the system drive

Apps

Applies to: Corporate and personal devices

User productivity on mobile devices is often driven by apps.

Windows 10 makes it possible to develop apps that work seamlessly across multiple devices using the Universal Windows Platform (UWP) for Windows apps. UWP converges the application platform for all devices running Windows 10 so that apps run without modification on all editions of Windows 10. This saves developers both time and resources, helping deliver apps to mobile users more quickly and efficiently. This write-once, run-anywhere model also boosts user productivity by providing a consistent, familiar app experience on any device type.

For compatibility with existing apps, Windows Phone 8.1 apps still run on Windows 10 Mobile devices, easing the migration to the newest platform. Microsoft recommend migrating your apps to UWP to take full advantage of the improvements in Windows 10 Mobile. In addition, bridges have been developed to easily and quickly update

existing Windows Phone 8.1 (Silverlight) and iOS apps to the UWP.

Microsoft also made it easier for organizations to license and purchase UWP apps via Microsoft Store for Business and deploy them to employee devices using the Microsoft Store, or an MDM system, that can be integrated with the Microsoft Store for Business. Putting apps into the hands of mobile workers is critical, but you also need an efficient way to ensure those apps comply with corporate policies for data security.

To learn more about Universal Windows apps, see the [Guide to Universal Windows Platform \(UWP\) apps](#) for additional information, or take this [Quick Start Challenge: Universal Windows Apps in Visual Studio](#). Also, see [Porting apps to Windows 10](#).

Microsoft Store for Business: Sourcing the right app

Applies to: Corporate and personal devices

The first step in app management is to obtain the apps your users need. You can develop your own apps or source your apps from the Microsoft Store. With Windows Phone 8.1, an MSA was needed to acquire and install apps from the Microsoft Store. With the Microsoft Store for Business, Microsoft enables organizations to acquire apps for employees from a private store with the Microsoft Store, without the need for MSAs on Windows 10 devices.

Microsoft Store for Business is a web portal that allows IT administrators to find, acquire, manage, and distribute apps to Windows 10 devices.

Azure AD authenticated managers have access to Microsoft Store for Business functionality and settings, and store managers can create a private category of apps that are specific and private to their organization. (You can get more details about what specific Azure AD accounts have access to Microsoft Store for Business here). Microsoft Store for Business enables organizations to purchase app licenses for their organization and make apps available to their employees. In addition to commercially available apps, your developers can publish line-of-business (LOB) apps to Microsoft Store for Business by request. You can also integrate their Microsoft Store for Business subscriptions with their MDM systems, so the MDM system can distribute and manage apps from Microsoft Store for Business.

Microsoft Store for Business supports app distribution under two licensing models: online and offline.

The online model (store-managed) is the recommended method, and supports both personal device and corporate device management scenarios. To install online apps, the device must have Internet access at the time of installation. On corporate devices, an employee can be authenticated with an Azure AD account to install online apps. On personal devices, an employee must register their device with Azure AD to be able to install corporate licensed online apps. Corporate device users will find company licensed apps in the Store app on their phone in a private catalog. When an MDM system is associated with the Store for Business, IT administrators can present Store apps within the MDM system app catalog where users can find and install their desired apps. IT administrators can also push required apps directly to employee devices without the employee's intervention.

Employees with personal devices can install apps licensed by their organization using the Store app on their device. They can use either the Azure AD account or Microsoft Account within the Store app if they wish to purchase personal apps. If you allow employees with corporate devices to add a secondary Microsoft Account (MSA), the Store app on the device provides a unified method for installing personal and corporate apps.

Online licensed apps do not need to be transferred or downloaded from the Microsoft Store to the MDM system to be distributed and managed. When an employee chooses a company-owned app, it will automatically be installed from the cloud. Also, apps will be automatically updated when a new version is available or can be removed if needed. When an app is removed from a device by the MDM system or the user, Microsoft Store for Business reclaims the license so it can be used for another user or on another device.

To distribute an app offline (organization-managed), the app must be downloaded from the Microsoft Store for Business. This can be accomplished in the Microsoft Store for Business portal by an authorized administrator. Offline licensing requires the app developer to opt-in to the licensing model, as the Microsoft Store is no longer able to track licenses for the developer. If the app developer doesn't allow download of the app from Microsoft

Store, then you must obtain the files directly from the developer or use the online licensing method.

To install acquired Microsoft Store or LOB apps offline on a Windows 10 Mobile device, IT administrators can use an MDM system. The MDM system distributes the app packages that you downloaded from Microsoft Store (also called sideloading) to Windows 10 Mobile devices. Support for offline app distribution depends on the MDM system you are using, so consult your MDM vendor documentation for details. You can fully automate the app deployment process so that no user intervention is required.

Microsoft Store apps or LOB apps that have been uploaded to the Microsoft Store for Business are automatically trusted on all Windows devices, as they are cryptographically signed with Microsoft Store certificates. LOB apps that are uploaded to the Microsoft Store for Business are private to your organization and are never visible to other companies or consumers. If you do not want to upload your LOB apps, you have to establish trust for the app on your devices. To establish this trust, you'll need to generate a signing certificate with your Public Key Infrastructure and add your chain of trust to the trusted certificates on the device (see the certificates section). You can install up to 20 self-signed LOB apps per device with Windows 10 Mobile. To install more than 20 apps on a device, you can purchase a signing certificate from a trusted public Certificate Authority, or upgrade your devices to Windows 10 Mobile Enterprise edition.

Learn more about the [Microsoft Store for Business](#).

Managing apps

Applies to: Corporate devices

IT administrators can control which apps are allowed to be installed on Windows 10 Mobile devices and how they should be kept up-to-date.

Windows 10 Mobile includes AppLocker, which enables administrators to create allow or disallow (sometimes also called whitelist/blacklist) lists of apps from the Microsoft Store. This capability extends to built-in apps, as well, such as Xbox, Groove, text messaging, email, and calendar, etc. The ability to allow or deny apps helps to ensure that people use their mobile devices for their intended purposes. However, it is not always an easy approach to find a balance between what employees need or request and security concerns. Creating allow or disallow lists also requires keeping up with the changing app landscape in the Microsoft Store.

For more details, see [AppLocker CSP](#).

In addition to controlling which apps are allowed, IT professionals can also implement additional app management settings on Windows 10 Mobile, using an MDM.

- **Allow All Trusted Apps** Whether users can sideload apps on the device.
- **Allow App Store Auto Update** Whether automatic updates of apps from Microsoft Store are allowed.
- **Allow Developer Unlock** Whether developer unlock is allowed.
- **Allow Shared User App Data** Whether multiple users of the same app can share data.
- **Allow Store** Whether Microsoft Store app is allowed to run. This will completely block the user from installing apps from the Store, but will still allow app distribution through an MDM system.
- **Application Restrictions** An XML blob that defines the app restrictions for a device. The XML blob can contain an app allow or deny list. You can allow or deny apps based on their app ID or publisher. See AppLocker above.
- **Disable Store Originated Apps** Disables the launch of all apps from Microsoft Store that came pre-installed or were downloaded before the policy was applied.
- **Require Private Store Only** Whether the private store is exclusively available to users in the Store app on the device. If enabled, only the private store is available. If disabled, the retail catalog and private store are both available.
- **Restrict App Data to System Volume** Whether app data is allowed only on the system drive or can be stored on an SD card.
- **Restrict App to System Volume** Whether app installation is allowed only to the system drive or can be

installed on an SD card.

- **Start screen layout** An XML blob used to configure the Start screen (see [Start layout for Windows 10 Mobile](#) for more information).

Find more details on application management options in the [Policy CSP](#)

Data leak prevention

Applies to: Corporate and personal devices

One of the biggest challenges in protecting corporate information on mobile devices is keeping that data separate from personal data. Most solutions available to create this data separation require users to login in with a separate username and password to a container that stores all corporate apps and data, an experience that degrades user productivity.

Windows 10 Mobile includes Windows Information Protection to transparently keep corporate data protected and personal data private. It automatically tags personal and corporate data and applies policies for those apps that can access data classified as corporate. This includes when data is at rest on local or removable storage. Because corporate data is always protected, users cannot copy it to public locations like social media or personal email.

Windows Information Protection works with all apps, which are classified into two categories: enlightened and unenlightened. Enlightened apps can differentiate between corporate and personal data, correctly determining which to protect based on policies. Corporate data will be encrypted at all times and attempts to copy/paste or share this information with non-corporate apps or users will fail. Unenlightened apps consider all data corporate and encrypt everything by default.

Any app developed on the UWA platform can be enlightened. Microsoft has made a concerted effort to enlighten several of its most popular apps, including:

- Microsoft Edge
- Microsoft People
- Mobile Office apps (Word, Excel, PowerPoint, and OneNote)
- Outlook Mail and Calendar
- Microsoft Photos
- Microsoft OneDrive
- Groove Music
- Microsoft Movies & TV
- Microsoft Messaging

The following table lists the settings that can be configured for Windows Information Protection:

- **Enforcement level*** Set the enforcement level for information protection:
 - Off (no protection)
 - Silent mode (encrypt and audit only)
 - Override mode (encrypt, prompt, and audit)
 - Block mode (encrypt, block, and audit)
- **Enterprise protected domain names*** A list of domains used by the enterprise for its user identities. User identities from one of these domains is considered an enterprise managed account and data associated with it should be protected.
- **Allow user decryption** Allows the user to decrypt files. If not allowed, the user will not be able to remove protection from enterprise content through the OS or app user experience.
- **Require protection under lock configuration** Specifies whether the protection under lock feature (also known as encrypt under PIN) should be configured.
- **Data recovery certificate*** Specifies a recovery certificate that can be used for data recovery of encrypted files. This is the same as the data recovery agent (DRA) certificate for encrypting file system (EFS), only

delivered through MDM instead of Group Policy.

- **Revoke on unenroll** Whether to revoke the information protection keys when a device unenrolls from the management service.
- **RMS template ID for information protection** Allows the IT admin to configure the details about who has access to RMS-protected files and for how long.
- **Allow Azure RMS for information protection** Specifies whether to allow Azure RMS encryption for information protection.
- **Show information protection icons** Determines whether overlays are added to icons for information protection secured files in web browser and enterprise-only app tiles in the Start menu.
- **Status** A read-only bit mask that indicates the current state of information protection on the device. The MDM service can use this value to determine the current overall state of information protection.
- **Enterprise IP Range*** The enterprise IP ranges that define the computers in the enterprise network. Data that comes from those computers will be considered part of the enterprise and protected.
- **Enterprise Network Domain Names*** the list of domains that comprise the boundaries of the enterprise. Data from one of these domains that is sent to a device will be considered enterprise data and protected.
- **Enterprise Cloud Resources** A list of Enterprise resource domains hosted in the cloud that need to be protected.

Note: * Are mandatory Windows Information Protection policies. To make Windows Information Protection functional, AppLocker and network isolation settings - specifically Enterprise IP Range and Enterprise Network Domain Names – must be configured. This defines the source of all corporate data that needs protection and also ensures data written to these locations won't be encrypted by the user's encryption key (so that others in the company can access it).

For more information on Windows Information Protection, see the [EnterpriseDataProtection CSP](#) and the following in-depth article series [Protect your enterprise data using Windows Information Protection](#).

Managing user activities

Applies to: Corporate devices

On corporate devices, some user activities expose corporate data to unnecessary risk. For example, users might create a screen capture of corporate information out of an internal LOB app. To mitigate the risk, you can restrict the Windows 10 Mobile user experience to help protect corporate data and prevent data leaks. The following demonstrates those capabilities that can be used to help prevent data leaks.

- **Allow copy and paste** Whether users can copy and paste content
- **Allow Cortana** Whether users can use Cortana on the device (where available)
- **Allow device discovery** Whether the device discovery user experience is available on the lock screen (for example, controlling whether a device could discover a projector [or other devices] when the lock screen is displayed)
- **Allow input personalization** Whether personally identifiable information can leave the device or be saved locally (e.g., Cortana learning, inking, dictation)
- **Allow manual MDM unenrollment** Whether users are allowed to delete the workplace account (i.e., unenroll the device from the MDM system)
- **Allow screen capture** Whether users are allowed to capture screenshots on the device
- **Allow SIM error dialog prompt** Specifies whether to display a dialog prompt when no SIM card is installed
- **Allow sync my settings** Whether the user experience settings are synchronized between devices (works with Microsoft accounts only)
- **Allow toasts notifications above lock screen** Whether users are able to view toast notification on the device lock screen
- **Allow voice recording** Whether users are allowed to perform voice recordings

- **Do Not Show Feedback Notifications** Prevents devices from showing feedback questions from Microsoft
- **Allow Task Switcher** Allows or disallows task switching on the device to prevent visibility of App screen tombstones in the task switcher
- **Enable Offline Maps Auto Update** Disables the automatic download and update of map data
- **Allow Offline Maps Download Over Metered Connection** Allows the download and update of map data over metered connections

You can find more details on the experience settings in Policy CSP.

Microsoft Edge

Applies to: Corporate and personal devices

MDM systems also give you the ability to manage Microsoft Edge on mobile devices. Microsoft Edge is the only browser available on Windows 10 Mobile devices. It differs slightly from the desktop version as it does not support Flash or Extensions. Edge is also an excellent PDF viewer as it can be managed and integrates with Windows Information Protection.

The following settings for Microsoft Edge on Windows 10 Mobile can be managed.

- **Allow Browser** Whether users can run Microsoft Edge on the device
- **Allow Do Not Track headers** Whether Do Not Track headers are allowed
- **Allow InPrivate** Whether users can use InPrivate browsing
- **Allow Password Manager** Whether users can use Password Manager to save and manage passwords locally
- **Allow Search Suggestions in Address Bar** Whether search suggestions are shown in the address bar
- **Allow SmartScreen** Whether SmartScreen Filter is enabled
- **Cookies** Whether cookies are allowed
- **Favorites** Configure Favorite URLs
- **First Run URL** The URL to open when a user launches Microsoft Edge for the first time
- **Prevent SmartScreen Prompt Override** Whether users can override the SmartScreen warnings for URLs
- **Prevent Smart Screen Prompt Override for Files** Whether users can override the SmartScreen warnings for files

Manage

In enterprise IT environments, the need for security and cost control must be balanced against the desire to provide users with the latest technologies. Since cyberattacks have become an everyday occurrence, it is important to properly maintain the state of your Windows 10 Mobile devices. IT needs to control configuration settings, keeping them from drifting out of compliance, as well as enforce which devices can access internal applications. Windows 10 Mobile delivers the mobile operations management capabilities necessary to ensure that devices are in compliance with corporate policy.

Servicing options

A streamlined update process

Applies to: Corporate and personal devices

Microsoft has streamlined the Windows product engineering and release cycle so new features, experiences, and functionality demanded by the market can be delivered more quickly than ever before. Microsoft plans to deliver two Feature Updates per year (12-month period). **Feature Updates** establish a Current Branch or CB, and have an associated version.

Branch	Version	Release Date
--------	---------	--------------

Current Branch	1511	November 2015
Current Branch for Business	1511	March 2016
Current Branch	1607	July 2016

Microsoft will also deliver and install monthly updates for security and stability directly to Windows 10 Mobile devices. These **Quality Updates**, released under Microsoft control via Windows Update, are available for all devices running Windows 10 Mobile. Windows 10 Mobile devices consume Feature Updates and Quality Updates as part of the same standard update process.

Quality Updates are usually smaller than Feature Updates, but the installation process and experience is very similar, though larger updates will take more time to install. Enterprise customers can manage the update experience and process on Windows 10 Mobile devices using an MDM system, after upgrading the devices to Enterprise edition. In most cases, policies to manage the update process will apply to both feature and quality updates.

Microsoft aspires to update Windows 10 Mobile devices with the latest updates automatically and without being disruptive for all customers. Out-of-the-box, a Windows 10 Mobile device will Auto Scan for available updates. However, depending on the device's network and power status, update methods and timing will vary.

Network connection	Description	Auto Scan	Auto Download	Auto Install	Auto Restart
Wi-Fi	Device is connected to a personal or corporate Wi-Fi network (no data charges)	Yes	Yes	Yes	Yes – outside of Active Hours (forced restart after 7 days if user postpones restart)
Cellular	Device is only connected to a cellular network (standard data charges apply)	Will skip a daily scan if scan was successfully completed in the last 5 days	Will only occur if update package is small and does not exceed the mobile operator data limit.	Yes	Idem
Cellular -- Roaming	Device is only connected to a cellular network and roaming charges apply	No	No	No	Idem

Keeping track of updates releases

Applies to: Corporate and Personal devices

Microsoft publishes new feature updates for Windows 10 and Windows 10 Mobile on a regular basis. The [Windows release information page](#) is designed to help you determine if your devices are current with the latest Windows 10 feature and quality updates. The release information published on this page, covers both Windows 10 for PCs and Windows 10 Mobile. In addition, the [Windows update history page](#) helps you understand what these updates are about.

Note: We invite IT Professionals to participate in the Windows Insider Program to test updates before they are officially released to make Windows 10 Mobile even better. If you find any issues, please send us feedback via the Feedback Hub

Windows as a Service

Applies to: Corporate and Personal devices

Microsoft created a new way to deliver and install updates to Windows 10 Mobile directly to devices without Mobile Operator approval. This capability helps to simplify update deployments and ongoing management, broadens the base of employees who can be kept current with the latest Windows features and experiences, and lowers total cost of ownership for organizations who no longer have to manage updates to keep devices secure.

Update availability depends on what servicing option you choose for the device. These servicing options are outlined in the chart below:

Servicing option	Availability of new features for installation	Minimum length of servicing lifetime	Key benefits	Supported editions
Windows Insider Builds	As appropriate during development cycle, released to Windows Insiders only	Variable, until the next Insider build is released to Windows Insiders	Allows Insiders to test new feature and application compatibility before a Feature Update is released	Mobile
Current Branch (CB)	Immediately after the Feature Update is published to Windows Update by Microsoft	Microsoft typically releases two Feature Updates per 12-month period (approximately every four months, though it can potentially be longer)	Makes new features available to users as soon as possible	Mobile & Mobile Enterprise
Current Branch for Business (CBB)	A minimum of four months after the corresponding Feature Update is first published to Windows Update by Microsoft	A minimum of four months, though it potentially can be longer	Provides additional time to test new feature before deployment	Mobile Enterprise only

Enterprise Edition

Applies to: Corporate devices

While Windows 10 Mobile provides updates directly to user devices from Windows Update, there are many organizations that want to track, test, and schedule updates to corporate devices. To support these requirements, we created the Windows 10 Mobile Enterprise edition.

Upgrading to Windows 10 Mobile Enterprise edition provides additional device and app management capabilities for organizations that want to:

- **Defer, approve and deploy feature and quality updates:** Windows 10 Mobile devices get updates directly from Windows Update. If you want to curate updates prior to deploying them, an upgrade to Windows 10 Mobile Enterprise edition is required. Once Enterprise edition is enabled, the phone can be set to the Current Branch for Business servicing option, giving IT additional time to test updates before they are released.
- **Deploy an unlimited number of self-signed LOB apps to a single device:** To use an MDM system to deploy LOB apps directly to devices, you must cryptographically sign the software packages with a code signing certificate that your organization's certificate authority (CA) generates. You can deploy a maximum of 20 self-signed LOB apps to a Windows 10 Mobile device. To deploy more than 20 self-signed LOB apps, Windows 10 Mobile Enterprise is required.

- **Set the diagnostic data level:** Microsoft collects diagnostic data to help keep Windows devices secure and to help Microsoft improve the quality of Windows and Microsoft services. An upgrade to Windows 10 Mobile Enterprise edition is required to set the diagnostic data level so that only diagnostic information required to keep devices secured is gathered.

To learn more about diagnostic, see [Configure Windows diagnostic data in your organization](#).

To activate Windows 10 Mobile Enterprise, use your MDM system or a provisioning package to inject the Windows 10 Enterprise license on a Windows 10 Mobile device. Licenses can be obtained from the Volume Licensing portal. For testing purposes, you can obtain a licensing file from the MSDN download center. A valid MSDN subscription is required.

Details on updating a device to Enterprise edition with [WindowsLicensing CSP](#)

Recommendation: Microsoft recommends using Enterprise edition only on corporate devices. Once a device has been upgraded, it cannot be downgraded. Even a device wipe or reset will not remove the enterprise license from personal devices.

Deferring and Approving Updates with MDM

Applies to: Corporate devices with Enterprise edition

Once a device is upgraded to Windows 10 Mobile Enterprise edition, you can manage devices that receive updates from Windows Update (or Windows Update for Business) with a set of update policies.

To control Feature Updates, you will need to move your devices to the Current Branch for Business (CBB) servicing option. A device that subscribes to CBB will wait for the next CBB to be published by Microsoft Update. While the device will wait for Feature Updates until the next CBB, Quality Updates will still be received by the device.

To control monthly Quality Update additional deferral policies, need to be set to your desired deferral period. When Quality Updates are available for your Windows 10 Mobile devices from Windows Update, these updates will not install until your deferral period lapses. This gives IT Professionals some time to test the impact of the updates on devices and apps.

Before updates are distributed and installed, you may want to test them for issues or application compatibility. IT pros have the ability require updates to be approved. This enables the MDM administrator to select and approve specific updates to be installed on a device and accept the EULA associated with the update on behalf of the user. Please remember that on Windows 10 Mobile all updates are packaged as a "OS updates" and never as individual fixes.

You may want to choose to handle Quality Updates and Feature Updates in the same way and not wait for the next CBB to be released to your devices. This streamlines the release of updates using the same process for approval and release. You can apply different deferral period by type of update. In version 1607 Microsoft added additional policy settings to enable more granularity to control over updates.

Once updates are being deployed to your devices, you may want to pause the rollout of updates to enterprise devices. For example, after you start rolling out a quality update, certain phone models are adversely impacted or users are reporting a specific LOB app is not connecting and updating a database. Problems can occur that did not surface during initial testing. IT professionals can pause updates to investigate and remediate unexpected issues.

The following table summarizes applicable update policy settings by version of Windows 10 Mobile. All policy settings are backward compatible, and will be maintained in future Feature Updates. Consult the documentation of your MDM system to understand support for these settings in your MDM.

Activity (Policy)	Version 1511 settings	Version 1607 settings
-------------------	-----------------------	-----------------------

Subscribe device to CBB, to defer Feature Updates	RequireDeferUpgrade Defers Feature Update until next CBB release. Device will receive quality updates from Current Branch for Business (CBB). Defers feature update for minimum of 4 months after Current Branch was release.	BranchReadinessLevel Defers Feature Update until next CBB release. Device will receive quality updates from Current Branch for Business (CBB). Defers feature update for minimum of 4 months after Current Branch was release.
Defer Updates	DeferUpdatePeriod Defer Quality Updates for 4 weeks or 28 days	DeferQualityUpdatePeriodInDays Defer Feature and Quality Updates for up to 30 days.
Approve Updates	RequireUpdateApproval	RequireUpdateApproval
Pause Update rollout once an approved update is being deployed, pausing the rollout of the update.	PauseDeferrals Pause Feature Updates for up to 35 days	PauseQualityUpdates Pause Feature Updates for up to 35 days

Managing the Update Experience

Applies to: Corporate devices with Enterprise edition

Set update client experience with [Allowautomaticupdate](#) policy for your employees. This allows the IT Pro to influence the way the update client on the devices behaves when scanning, downloading, and installing updates.

This can include:

- Notifying users prior to downloading updates.
- Automatically downloading updates, and then notifying users to schedule a restart (this is the default behavior if this policy is not configured).
- Automatically downloading and restarting devices with user notification.
- Automatically downloading and restarting devices at a specified time.
- Automatically downloading and restarting devices without user interaction.
- Turning off automatic updates. This option should be used only for systems under regulatory compliance. The device will not receive any updates.

In addition, in version 1607, you can configure when the update is applied to the employee device to ensure updates installs or reboots don't interrupt business or worker productivity. Update installs and reboots can be scheduled [outside of active hours](#) (supported values are 0-23, where 0 is 12am, 1 is 1am, etc.) or on a specific what [day of the week](#) (supported values are 0-7, where 0 is every day, 1 is Sunday, 2 is Monday, etc.).

Managing the source of updates with MDM

Applies to: Corporate devices with Enterprise edition

Although Windows 10 Enterprise enables IT administrators to defer installation of new updates from Windows Update, enterprises may also want additional control over update processes. With this in mind, Microsoft created Windows Update for Business. Microsoft designed Windows Update for Business to provide IT administrators with additional Windows Update-centric management capabilities, such as the ability to deploy updates to groups of devices and to define maintenance windows for installing updates. If you are using a MDM system, the use of Windows Update for Business is not a requirement, as you can manage these features from your MDM system.

Learn more about [Windows Update for Business](#).

IT administrators can specify where the device gets updates from with AllowUpdateService. This could be

Microsoft Update, Windows Update for Business, or Windows Server Update Services (WSUS).

Managing Updates with Windows Update Server

Applies to: Corporate devices with Enterprise edition

When using WSUS, set **UpdateServiceUrl** to allow the device to check for updates from a WSUS server instead of Windows Update. This is useful for on-premises MDMs that need to update devices that cannot connect to the Internet, usually handheld devices used for task completion, or other Windows IoT devices.

Learn more about [managing updates with Windows Server Update Services \(WSUS\)](#)

Querying the device update status

Applies to: Personal and corporate devices

In addition to configuring how Windows 10 Mobile Enterprise obtains updates, the MDM administrator can query devices for Windows 10 Mobile update information so that update status can be checked against a list of approved updates.

The device update status query provides an overview of:

- Installed updates: A list of updates that are installed on the device.
- Installable updates: A list of updates that are available for installation.
- Failed updates: A list of updates that failed during installation, including indication of why the update failed.
- Pending reboot: A list of updates that require a restart to complete update installation.
- Last successful scan time: The last time a successful update scan was completed.
- Defer upgrade: Whether the upgrade is deferred until the next update cycle.

Device health

Applies to: Personal and corporate devices

Device Health Attestation (DHA) is another line of defense that is new to Windows 10 Mobile. It can be used to remotely detect devices that lack a secure configuration or have vulnerabilities that could allow them to be easily exploited by sophisticated attacks.

Windows 10 Mobile makes it easy to integrate with Microsoft Intune or third-party MDM solutions for an overall view of device health and compliance. Using these solutions together, you can detect jailbroken devices, monitor device compliance, generate compliance reports, alert users or administrators to issues, initiate corrective action, and manage conditional access to resources like Office 365 or VPN.

The first version of Device Health Attestation (DHA) was released in June 2015 for Windows 10 devices that supported TPM 2.0 and operated in an enterprise cloud-based topology. In the Windows 10 anniversary release, Device Health Attestation (DHA) capabilities are extended to legacy devices that support TPM 1.2, hybrid, and on-premises environments that have access to the Internet or operate in an air-gapped network.

The health attestation feature is based on Open Mobile Alliance (OMA) standards. IT managers can use DHA to validate devices that:

- Run Windows 10 operating system (mobile phone or PC)
- Support Trusted Module Platform (TPM 1.2 or 2.0) in discrete or firmware format
- Are managed by a DHA-enabled device management solution (Intune or third-party MDM)
- Operate in cloud, hybrid, on-premises, and BYOD scenarios

DHA-enabled device management solutions help IT managers create a unified security bar across all managed Windows 10 Mobile devices. This allows IT managers to:

- Collect hardware attested data (highly assured) data remotely

- Monitor device health compliance and detect devices that are vulnerable or could be exploited by sophisticated attacks
- Take actions against potentially compromised devices, such as:
 - Trigger corrective actions remotely so offending device is inaccessible (lock, wipe, or brick the device)
 - Prevent the device from getting access to high-value assets (conditional access)
 - Trigger further investigation and monitoring (route the device to a honeypot for further monitoring)
 - Simply alert the user or the admin to fix the issue

Note: Windows Device Health Attestation Service can be used for conditional access scenarios which may be enabled by Mobile Device Management solutions (e.g.: Microsoft Intune) and other types of management systems (e.g.: SCCM) purchased separately.

For more information about health attestation in Windows 10 Mobile, see the [Windows 10 Mobile security guide](#).

This is a list of attributes that are supported by DHA and can trigger the corrective actions mentioned above.

- **Attestation Identity Key (AIK) present** Indicates that an AIK is present (i.e., the device can be trusted more than a device without an AIK).
- **Data Execution Prevention (DEP) enabled** Whether a DEP policy is enabled for the device, indicating that the device can be trusted more than a device without a DEP policy.
- **BitLocker status** BitLocker helps protect the storage on the device. A device with BitLocker can be trusted more than a device without BitLocker.
- **Secure Boot enabled** Whether Secure Boot is enabled on the device. A device with Secure Boot enabled can be trusted more than a device without Secure Boot. Secure Boot is always enabled on Windows 10 Mobile devices.
- **Code integrity enabled** Whether the code integrity of a drive or system file is validated each time it's loaded into memory. A device with code integrity enabled can be trusted more than a device without code integrity.
- **Safe mode** Whether Windows is running in safe mode. A device that is running Windows in safe mode isn't as trustworthy as a device running in standard mode.
- **Boot debug enabled** Whether the device has boot debug enabled. A device that has boot debug enabled is less secure (trusted) than a device without boot debug enabled.
- **OS kernel debugging enabled** Whether the device has operating system kernel debugging enabled. A device that has operating system kernel debugging enabled is less secure (trusted) than a device with operating system kernel debugging disabled.
- **Test signing enabled** Whether test signing is disabled. A device that has test signing disabled is more trustworthy than a device that has test signing enabled.
- **Boot Manager Version** The version of the Boot Manager running on the device. The HAS can check this version to determine whether the most current Boot Manager is running, which is more secure (trusted).
- **Code integrity version** Specifies the version of code that is performing integrity checks during the boot sequence. The HAS can check this version to determine whether the most current version of code is running, which is more secure (trusted).
- **Secure Boot Configuration Policy (SBCP) present** Whether the hash of the custom SBCP is present. A device with an SBCP hash present is more trustworthy than a device without an SBCP hash.
- **Boot cycle whitelist** The view of the host platform between boot cycles as defined by the manufacturer compared to a published whitelist. A device that complies with the whitelist is more trustworthy (secure) than a device that is noncompliant.

Example scenario

Windows 10 mobile has protective measures that work together and integrate with Microsoft Intune or third-party Mobile Device Management (MDM) solutions. IT administrators can monitor and verify compliance to ensure corporate resources are protected end-to-end with the security and trust rooted in the physical hardware

of the device.

Here is what occurs when a smartphone is turned on:

1. Windows 10 Secure Boot protects the boot sequence, enables the device to boot into a defined and trusted configuration, and loads a factory trusted boot loader.
2. Windows 10 Trusted Boot takes control, verifies the digital signature of the Windows kernel, and the components are loaded and executed during the Windows startup process.
3. In parallel to Steps 1 and 2, Windows 10 Mobile TPM (Trusted Platform Modules – measured boot) runs independently in a hardware-protected security zone (isolated from boot execution path monitors boot activities) to create an integrity protected and tamper evident audit trail - signed with a secret that is only accessible by TPM.
4. Devices managed by a DHA-enabled MDM solution send a copy of this audit trail to Microsoft Health Attestation Service (HAS) in a protected, tamper-resistant, and tamper-evident communication channel.
5. Microsoft HAS reviews the audit trails, issues an encrypted/signed report, and forwards it to the device.
6. IT managers can use a DHA-enabled MDM solution to review the report in a protected, tamper-resistant and tamper-evident communication channel. They can assess if a device is running in a compliant (healthy) state, allow access, or trigger corrective action aligned with security needs and enterprise policies.

Asset reporting

Applies to: Corporate devices with Enterprise edition

Device inventory helps organizations better manage devices because it provides in-depth information about those devices. MDM systems collect inventory information remotely and provide reporting capabilities to analyze device resources and information. This data informs IT about the current hardware and software resources of the device (e.g., installed updates).

The following list shows examples of the Windows 10 Mobile software and hardware information that a device inventory provides. In addition to this information, the MDM system can read any of the configuration settings described in this guide.

- **Installed enterprise apps** List of the enterprise apps installed on the device
- **Device name** The device name configured for the device
- **Firmware version** Version of firmware installed on the device
- **Operating system version** Version of the operating system installed on the device
- **Device local time** Local time on the device
- **Processor type** Processor type for the device
- **Device model** Model of the device as defined by the manufacturer
- **Device manufacturer** Manufacturer of the device
- **Device processor architecture** Processor architecture for the device
- **Device language** Language in use on the device
- **Phone number** Phone number assigned to the device
- **Roaming status** Indicates whether the device has a roaming cellular connection
- ****International mobile equipment identity (IMEI) and international mobile subscriber identity (IMSI)** Unique identifiers for the cellular connection for the phone; Global System for Mobile Communications networks identify valid devices by using the IMEI, and all cellular networks use the IMSI to identify the device and user
- **Wi-Fi IP address** IPv4 and IPv6 addresses currently assigned to the Wi-Fi adapter in the device
- **Wi-Fi media access control (MAC) address** MAC address assigned to the Wi-Fi adapter in the device
- **Wi-Fi DNS suffix and subnet mask** DNS suffix and IP subnet mask assigned to the Wi-Fi adapter in the device
- **Secure Boot state** Indicates whether Secure Boot is enabled
- **Enterprise encryption policy compliance** Indicates whether the device is encrypted

Manage diagnostic data

Applies to: Corporate devices with Windows 10 Mobile Enterprise edition

Microsoft uses diagnostics, performance, and usage data from Windows devices to help inform decisions and focus efforts to provide the most robust and valuable platform for your business and the people who count on Windows to enable them to be as productive as possible. Diagnostic data helps keep Windows devices healthy, improve the operating system, and personalize features and services.

You can control the level of data that diagnostic data systems collect. To configure devices, specify one of these levels in the Allow Telemetry setting with your MDM system.

For more information, see [Configure Windows diagnostic data in Your organization](#).

Note: Diagnostic data can only be managed when the device is upgraded to Windows 10 Mobile Enterprise edition.

Remote assistance

Applies to: Personal and corporate devices

The remote assistance features in Windows 10 Mobile help resolve issues that users might encounter even when the help desk does not have physical access to the device. These features include:

- **Remote lock** Support personnel can remotely lock a device. This ability can help when a user loses his or her mobile device and can retrieve it, but not immediately (e.g., leaving the device at a customer site).
- **Remote PIN reset** Support personnel can remotely reset the PIN, which helps when users forget their PIN and are unable to access their device. No corporate or user data is lost and users are able to quickly gain access to their devices.
- **Remote ring** Support personnel can remotely make devices ring. This ability can help users locate misplaced devices and, in conjunction with the Remote Lock feature, help ensure that unauthorized users are unable to access the device if they find it.
- **Remote find** Support personnel can remotely locate a device on a map, which helps identify the geographic location of the device. Remote find parameters can be configured via phone settings (see table below). The remote find feature returns the most current latitude, longitude, and altitude of the device.

Remote assistance policies

- **Desired location accuracy** The desired accuracy as a radius value in meters; has a value between 1 and 1,000 meters
- **Maximum remote find** Maximum length of time in minutes that the server will accept a successful remote find; has a value between 0 and 1,000 minutes
- **Remote find timeout** The number of seconds devices should wait for a remote find to finish; has a value between 0 and 1,800 seconds

These remote management features help organizations reduce the IT effort required to manage devices. They also help users quickly regain use of their device should they misplace it or forget the device password.

Remote control software Microsoft does not provide build-in remote control software, but works with partners to deliver these capabilities and services. With version 1607, remote assistant and control applications are available in the Microsoft Store.

Retire

Applies to: Corporate and Personal devices

Device retirement is the last phase of the device lifecycle, which in today's business environment averages about

18 months. After that time period, employees want the productivity and performance improvements that come with the latest hardware. It's important that devices being replaced with newer models are securely retired since you don't want any company data to remain on discarded devices that could compromise the confidentiality of your data. This is typically not a problem with corporate devices, but it can be more challenging in a personal device scenario. You need to be able to selectively wipe all corporate data without impacting personal apps and data on the device. IT also needs a way to adequately support users who need to wipe devices that are lost or stolen.

Windows 10 Mobile IT supports device retirement in both personal and corporate scenarios, allowing IT to be confident that corporate data remains confidential and user privacy is protected.

Note: All these MDM capabilities are in addition to the device's software and hardware factory reset features, which employees can use to restore devices to their factory configuration.

Personal devices: Windows 10 mobile supports the USA regulatory requirements for a "kill switch" in case your phone is lost or stolen. Reset protection is a free service on account.microsoft.com that helps ensure that the phone cannot be easily reset and reused. All you need to do to turn on **Reset Protection** is sign in with your Microsoft account and accept the recommended settings. To manually turn it on, you can find it under Settings > Updates & security > Find my phone. At this point, Reset Protection is only available with an MSA, not with Azure AD account. It is also only available in the USA and not in other regions of the world.

If you choose to completely wipe a device when lost or when an employee leaves the company, make sure you obtain consent from the user and follow any local legislation that protects the user's personal data.

A better option than wiping the entire device is to use Windows Information Protection to clean corporate-only data from a personal device. As explained in the Apps chapter, all corporate data will be tagged and when the device is unenrolled from your MDM system of your choice, all enterprise encrypted data, apps, settings and profiles will immediately be removed from the device without affecting the employee's existing personal data. A user can initiate unenrollment via the settings screen or unenrollment action can be taken by IT from within the MDM management console. Unenrollment is a management event and will be reported to the MDM system.

Corporate device: You can certainly remotely expire the user's encryption key in case of device theft, but please remember that will also make the encrypted data on other Windows devices unreadable for the user. A better approach for retiring a discarded or lost device is to execute a full device wipe. The help desk or device users can initiate a full device wipe. When the wipe is complete, Windows 10 Mobile returns the device to a clean state and restarts the OOB process.

Settings for personal or corporate device retirement

- **Allow manual MDM unenrollment** Whether users are allowed to delete the workplace account (i.e., unenroll the device from the MDM system)
- **Allow user to reset phone** Whether users are allowed to use Settings or hardware key combinations to return the device to factory defaults

Related topics

- [Mobile device management](#)
- [Enterprise Mobility + Security](#)
- [Overview of Mobile Device Management for Office 365](#)
- [Microsoft Store for Business](#)

Revision History

- November 2015 Updated for Windows 10 Mobile (version 1511)

- August 2016 Updated for Windows 10 Mobile Anniversary Update (version 1607)

Windows libraries

6/18/2019 • 6 minutes to read • [Edit Online](#)

Applies to: Windows 10, Windows 8.1, Windows 7, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2

Libraries are virtual containers for users' content. A library can contain files and folders stored on the local computer or in a remote storage location. In Windows Explorer, users interact with libraries in ways similar to how they would interact with other folders. Libraries are built upon the legacy known folders (such as My Documents, My Pictures, and My Music) that users are familiar with, and these known folders are automatically included in the default libraries and set as the default save location.

Features for Users

Windows libraries are backed by full content search and rich metadata. Libraries offer the following advantages to users:

- Aggregate content from multiple storage locations into a single, unified presentation.
- Enable users to stack and group library contents based on metadata.
- Enable fast, full-text searches across multiple storage locations, from Windows Explorer or from the Start menu.
- Support customized filter search suggestions, based on the types of files contained in the library.
- Enable users to create new libraries and specify which folders they want to include.

Features for Administrators

Administrators can configure and control Windows libraries in the following ways:

- Create custom libraries by creating and deploying Library Description (*.library-ms) files.
- Hide or delete the default libraries. (The Library node itself cannot be hidden or deleted from the Windows Explorer navigation pane.)
- Specify a set of libraries available to Default User, and then deploy those libraries to users that derive from Default User.
- Specify locations to include in a library.
- Remove a default location from a library.
- Remove advanced libraries features, when the environment does not support the local caching of files, by using the [Turn off Windows Libraries features that rely on indexed file data](#) Group Policy. This makes all libraries basic (see [Indexing Requirements and Basic Libraries](#)), removes libraries from the scope of the Start menu search, and removes other features to avoid confusing users and consuming resources.

More about Libraries

The following is important information about libraries you may need to understand to successfully manage your enterprise.

Library Contents

Including a folder in a library does not physically move or change the storage location of the files or folders; the library is a view into those folders. However, users interacting with files in a library are copying, moving, and deleting the files themselves, not copies of these files.

Default Libraries and Known Folders

The default libraries include:

- Documents
- Music
- Pictures
- Videos

Libraries are built upon the legacy known folders (such as My Documents, My Pictures, and My Music) that users are familiar with. These known folders are automatically included in the default libraries and set as the default save location. That is, when users drag, copy, or save a file to the Documents library, the file is moved, copied, or saved to the My Documents folder. Administrators and users can change the default save-to location.

Hiding Default Libraries

Users or administrators can hide or delete the default libraries, though the libraries node in the Navigation pane cannot be hidden or deleted. Hiding a default library is preferable to deleting it, as applications like Windows Media Player rely on the default libraries and will re-create them if they do not exist on the computer. See [How to Hide Default Libraries](#) for instructions.

Default Save Locations for Libraries

Each library has a default save location. Files are saved or copied to this location if the user chooses to save or copy a file to a library, rather than a specific location within the library. Known folders are the default save locations; however, users can select a different save location. If the user removes the default save location from a library, the next location is automatically selected as the new default save location. If the library is empty of locations or if all included locations cannot be saved to, then the save operation fails.

Indexing Requirements and “Basic” Libraries

Certain library features depend on the contents of the libraries being indexed. Library locations must be available for local indexing or be indexed in a manner conforming to the Windows Indexing Protocol. If indexing is not enabled for one or more locations within a library, the entire library reverts to basic functionality:

- No support for metadata browsing via **Arrange By** views.
- Grep-only searches.
- Grep-only search suggestions. The only properties available for input suggestions are **Date Modified** and **Size**.
- No support for searching from the Start menu. Start menu searches do not return files from basic libraries.
- No previews of file snippets for search results returned in Content mode.

To avoid this limited functionality, all locations within the library must be indexable, either locally or remotely. When users add local folders to libraries, Windows adds the location to the indexing scope and indexes the contents. Remote locations that are not indexed remotely can be added to the local index using Offline File synchronization. This gives the user the benefits of local storage even though the location is remote. Making a folder “Always available offline” creates a local copy of the folder’s files, adds those files to the index, and keeps the local and remote copies in sync. Users can manually sync locations which are not indexed remotely and are not using folder redirection to gain the benefits of being indexed locally.

For instructions on enabling indexing, see [How to Enable Indexing of Library Locations](#).

If your environment does not support caching files locally, you should enable the [Turn off Windows Libraries features that rely on indexed file](#) data Group Policy. This makes all libraries basic. For further information, see [Group Policy for Windows Search, Browse, and Organize](#).

Folder Redirection

While library files themselves cannot be redirected, you can redirect known folders included in libraries by using

Folder Redirection. For example, you can redirect the “My Documents” folder, which is included in the default Documents library. When redirecting known folders, you should make sure that the destination is either indexed or always available offline in order to maintain full library functionality. In both cases, the files for the destination folder are indexed and supported in libraries. These settings are configured on the server side.

Supported storage locations

The following table show which locations are supported in Windows libraries.

SUPPORTED LOCATIONS	UNSUPPORTED LOCATIONS
Fixed local volumes (NTFS/FAT)	Removable drives
Shares that are indexed (departmental servers*, Windows home PCs)	Removable media (such as DVDs) Network shares that are accessible through DFS Namespaces or are part of a failover cluster
Shares that are available offline (redirected folders that use Offline Files)	Network shares that aren't available offline or remotely indexed Network Attached Storage (NAS) devices
	Other data sources: SharePoint, Exchange, etc.

* For shares that are indexed on a departmental server, Windows Search works well in workgroups or on a domain server that has similar characteristics to a workgroup server. For example, Windows Search works well on a single share departmental server with the following characteristics:

- Expected maximum load is four concurrent query requests.
- Expected indexing corpus is a maximum of one million documents.
- Users directly access the server. That is, the server is not made available through DFS Namespaces.
- Users are not redirected to another server in case of failure. That is, server clusters are not used.

Library Attributes

The following library attributes can be modified within Windows Explorer, the Library Management dialog, or the Library Description file (*.library-ms):

- Name
- Library locations
- Order of library locations
- Default save location

The library icon can be modified by the administrator or user by directly editing the Library Description schema file.

See the [Library Description Schema](#) topic on MSDN for information on creating Library Description files.

See also

Concepts

- [Windows Search Features](#)
- [Windows Indexing Features](#)
- [Federated Search Features](#)
- [Administrative How-to Guides](#)

- [Group Policy for Windows Search, Browse, and Organize](#)
- [Additional Resources for Windows Search, Browse, and Organization](#)

Other resources

- [Folder Redirection, Offline Files, and Roaming User Profiles](#)
- [Library Description Schema](#)

Troubleshoot Windows 10 clients

6/18/2019 • 2 minutes to read • [Edit Online](#)

This section contains advanced troubleshooting topics and links to help you resolve issues with Windows 10 clients. Additional topics will be added as they become available.

Troubleshooting support topics

- [Advanced troubleshooting for Windows networking](#)
 - [Advanced troubleshooting wireless network connectivity](#)
 - [Advanced troubleshooting 802.1X authentication](#)
 - [Data collection for troubleshooting 802.1X authentication](#)
 - [Advanced troubleshooting for TCP/IP](#)
 - [Collect data using Network Monitor](#)
 - [Troubleshoot TCP/IP connectivity](#)
 - [Troubleshoot port exhaustion](#)
 - [Troubleshoot Remote Procedure Call \(RPC\) errors](#)
- [Advanced troubleshooting for Windows startup](#)
 - [Advanced troubleshooting for Windows boot problems](#)
 - [Advanced troubleshooting for Windows-based computer issues](#)
 - [Advanced troubleshooting for stop errors or blue screen errors](#)
 - [Advanced troubleshooting for stop error 7B or Inaccessible_Boot_Device](#)

Windows 10 update history

Microsoft regularly releases both updates and solutions for Windows 10. To ensure your computers can receive future updates, including security updates, it's important to keep them updated. Check out the following links for a complete list of released updates:

- [Windows 10 version 1809 update history](#)
- [Windows 10 version 1803 update history](#)
- [Windows 10 version 1709 update history](#)
- [Windows 10 Version 1703 update history](#)
- [Windows 10 Version 1607 update history](#)
- [Windows 10 Version 1511 update history](#)

These are the top Microsoft Support solutions for the most common issues experienced when using Windows 10 in an enterprise or IT pro environment. The links below include links to KB articles, updates, and library articles.

Solutions related to installing Windows Updates

- [How does Windows Update work](#)
- [Windows Update log files](#)
- [Windows Update troubleshooting](#)
- [Windows Update common errors and mitigation](#)
- [Windows Update - additional resources](#)

Solutions related to installing or upgrading Windows

- [Quick Fixes](#)
- [Troubleshooting upgrade errors](#)
- [Resolution procedures](#)
- [0xc1800118 error when you push Windows 10 Version 1607 by using WSUS](#)
- [0xC1900101 error when Windows 10 upgrade fails after the second system restart](#)

Solutions related to BitLocker

- [BitLocker recovery guide](#)
- [BitLocker: How to enable Network Unlock](#)
- [BitLocker: Use BitLocker Drive Encryption Tools to manage BitLocker](#)
- [BitLocker Group Policy settings](#)

Solutions related to Bugchecks or Stop Errors

- [Troubleshooting Stop error problems for IT Pros](#)
- [How to use Windows Recovery Environment \(WinRE\) to troubleshoot common startup issues](#)
- [How to troubleshoot Windows-based computer freeze issues](#)
- [Introduction of page file in Long-Term Servicing Channel and Semi-Annual Channel of Windows](#)

Solutions related to Windows Boot issues

- [Troubleshooting Windows boot problems for IT Pros](#)
- [How to use Windows Recovery Environment \(WinRE\) to troubleshoot common startup issues](#)

Solutions related to configuring or managing the Start menu

- [Manage Windows 10 Start and taskbar layout](#)
- [Customize and export Start layout](#)
- [Changes to Group Policy settings for Windows 10 Start](#)
- [Preinstalled system applications and Start menu may not work when you upgrade to Windows 10, Version 1511](#)
- [Start menu shortcuts aren't immediately accessible in Windows Server 2016](#)
- [Troubleshoot problems opening the Start menu or Cortana](#)
- [Modern apps are blocked by security software when you start the applications on Windows 10 Version 1607](#)

Solutions related to wireless networking and 802.1X authentication

- [Advanced Troubleshooting Wireless Network](#)
- [Advanced Troubleshooting 802.1x Authentication](#)
- [Troubleshooting Windows 802.11 Wireless Connections](#)
- [Troubleshooting Windows Secure 802.3 Wired Connections](#)
- [Windows 10 devices can't connect to an 802.1X environment](#)

Advanced troubleshooting for Windows networking

6/18/2019 • 2 minutes to read • [Edit Online](#)

The following topics are available to help you troubleshoot common problems related to Windows networking.

- [Advanced troubleshooting for wireless network connectivity](#)
- [Advanced troubleshooting 802.1X authentication](#)
 - [Data collection for troubleshooting 802.1X authentication](#)
- [Advanced troubleshooting for TCP/IP](#)
 - [Collect data using Network Monitor](#)
 - [Troubleshoot TCP/IP connectivity](#)
 - [Troubleshoot port exhaustion issues](#)
 - [Troubleshoot Remote Procedure Call \(RPC\) errors](#)

Concepts and technical references

[802.1X authenticated wired access overview](#)

[802.1X authenticated wireless access overview](#)

[Wireless access deployment overview](#)

[TCP/IP technical reference](#)

[Network Monitor](#)

[RPC and the network](#)

[How RPC works](#)

[NPS reason codes](#)

Advanced troubleshooting wireless network connectivity

6/18/2019 • 11 minutes to read • [Edit Online](#)

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](#).

Overview

This is a 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 is not meant to be representative of every wireless problem scenario.

Wireless ETW is incredibly verbose and calls out a lot of innocuous errors (rather flagged behaviors that have little or nothing to do with the problem scenario). Simply 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 is 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 at an elevated command prompt:

```
netsh trace start wireless_dbg capture=yes overwrite=yes maxsize=4096 tracefile=c:\tmp\wireless.etl
```

2. Reproduce the issue.

- If there is a failure to establish connection, try to manually connect.
- If it is 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:

```
netsh trace stop
```

4. To convert the output file to text format:

```
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 will have three files: wireless.cab, wireless.etl, and wireless.txt.

Troubleshooting

The following is a high-level view of the main wifi components in Windows.

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.

<p>WLAN Autoconfig Service (WlanSvc)</p>	<p>The WLAN Autoconfig Service (WlanSvc) handles the following core functions of wireless networks in windows:</p> <ul style="list-style-type: none"> • Scanning for wireless networks in range • Managing connectivity of wireless networks
<p>Media Specific Module (MSM)</p>	<p>The Media Specific Module (MSM) handles security aspects of connection being established.</p>
<p>Native Wifi stack</p>	<p>The Native Wifi stack consists of drivers and wireless APIs to interact with wireless miniports and the supporting user-mode Wlansvc.</p>
<p>Wifi miniport</p>	<p>Third-party wireless miniport drivers interface with the upper wireless stack to provide notifications to and receive commands from Windows.</p>

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.

The following is an example of a good connection setup:

```

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

```

The following is an example of a failed connection setup:

```

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 just prior to the last known good state.

Examining **[Microsoft-Windows-WLAN-AutoConfig]** logs just 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 their own individual state machines which follow specific transitions. Enable the **FSM transition**, **SecMgr Transition**, and **AuthMgr Transition** filters in TextAnalysisTool for more detail.

Continuing with the example above, the combined filters look like this:

```
[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 just 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:


```

[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 are Windows native wifi drivers which talk to the wifi miniport drivers. It is responsible for converting Wi-Fi (802.11) packets to 802.3 (Ethernet) so that TCP/IP and other protocols and can use it.

Enable trace filter for **[Microsoft-Windows-NWifi]:**

```

[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:

```
[0]0000.0000::08/28/17-13:24:29.127 [Microsoft-Windows-NWiFi]DisAssoc: 0x8A1514B62510 Reason: 0x4
```

This 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 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 would be done by examining internal logging/tracing from the AP.

Resources

[802.11 Wireless Tools and Settings](#)

[Understanding 802.1X authentication for wireless networks](#)

Example ETW capture

```

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 clicking **File > Load Filters**.

```

<?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**.

wireless.txt - [No filter file] - TextAnalysisTool.NET

File Edit View Filters Help

```
36873 [5]11C0.B878::2019-01-11 11:44:11.820 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Disconnected to State: Reset
37934 [8]11C0.98E0::2019-01-11 11:44:11.822 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Reset to State: Inv_Configuring
39008 [3]11C0.98E0::2019-01-11 11:44:11.854 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Inv_Configuring to State: Configuring
39395 [8]11C0.3370::2019-01-11 11:44:11.859 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Configuring to State: Associating
39973 [6]11C0.98E0::2019-01-11 11:44:12.039 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Associating to State: Authenticating
41533 [6]11C0.3370::2019-01-11 11:44:12.112 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Authenticating to State: Connected
```

36873 [5]11C0.B878::2019-01-11 11:44:11.820 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Disconnected to State: Reset

37934 [8]11C0.98E0::2019-01-11 11:44:11.822 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Reset to State: Inv_Configuring

39008 [3]11C0.98E0::2019-01-11 11:44:11.854 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Inv_Configuring to State: Configuring

39395 [8]11C0.3370::2019-01-11 11:44:11.859 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Configuring to State: Associating

39973 [6]11C0.98E0::2019-01-11 11:44:12.039 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Associating to State: Authenticating

41533 [6]11C0.3370::2019-01-11 11:44:12.112 [Microsoft-Windows-WLAN-AutoConfig]FSM Transition from State: Authenticating to State: Connected

Modifiers Pattern

Modifiers	Pattern
<input checked="" type="checkbox"/> a	FSM transition

Source: C:\tmp\wireless.txt Sel: 1 Fil: 6 Total: 209338 120 %

Filter: Matches text Text Color: [Default] Background: [Default]

Text: FSM transition

Description:

Excluding [!] Case-sensitive [Aa] Regular expression [R]

OK Cancel

Description	Hits
	6

Advanced troubleshooting 802.1X authentication

6/18/2019 • 3 minutes to read • [Edit Online](#)

Overview

This is a general troubleshooting of 802.1X wireless and wired clients. With 802.1X and wireless troubleshooting, it's important to know how the flow of authentication works, and then figuring out where it's breaking. It involves a lot of third party devices and software. Most of the time, we have to identify where the problem is, and another vendor has to fix it. Since we don't make access points or switches, it won't be an end-to-end Microsoft solution.

Scenarios

This troubleshooting technique applies to any scenario in which wireless or wired connections with 802.1X authentication is attempted and then fails to establish. The workflow covers Windows 7 - 10 for clients, and Windows Server 2008 R2 - 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 on 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 are not seeing both success and failure events, see the section below on [NPS audit policy](#).

Check Windows Security Event log on the NPS Server for NPS events corresponding to rejected ([event ID 6273](#)) or accepted ([event ID 6272](#)) connection attempts.

In the event message, scroll to the very bottom, and check the [Reason Code](#) field and the text associated with it.

```
Log Name: Security
Source: Microsoft Windows Security   Logged: MM/DD/YYYY hh:mm:ss
Event ID: 6273                       Task Category: Network Policy Server
Level: Information                    Keywords: Audit Failure

Network Policy Server denied 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.
    Reason Code:                   16
    Reason:                        Authentication failed due to a user credentials mismatch.
    Either the user name provided does not map to an existing user account or the password was incorrect.
```

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.

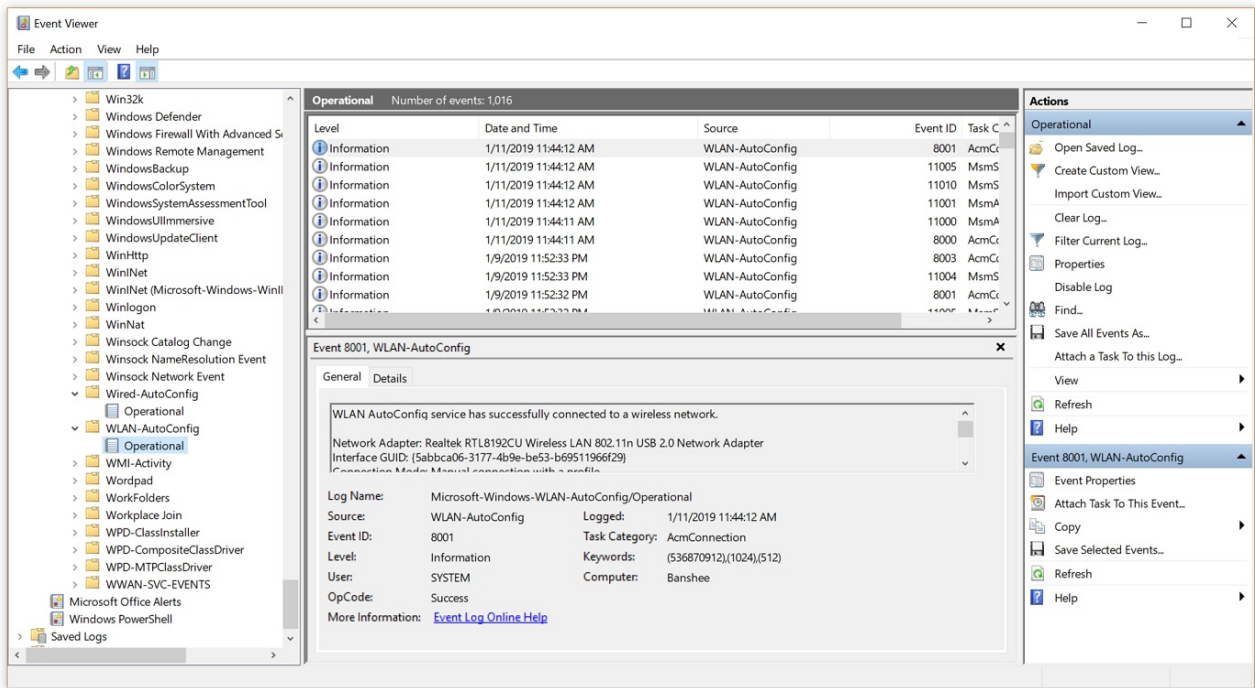
....

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, in the event of connectivity problems, the reason for the failure. For wired network access, Wired AutoConfig operational log is equivalent one.

On the client side, navigate to **Event Viewer (Local)\Applications and Services Logs\Microsoft\Windows\WLAN-AutoConfig/Operational** for wireless issues. For wired network access issues, navigate to **..\Wired-AutoConfig/Operational**. See the following example:

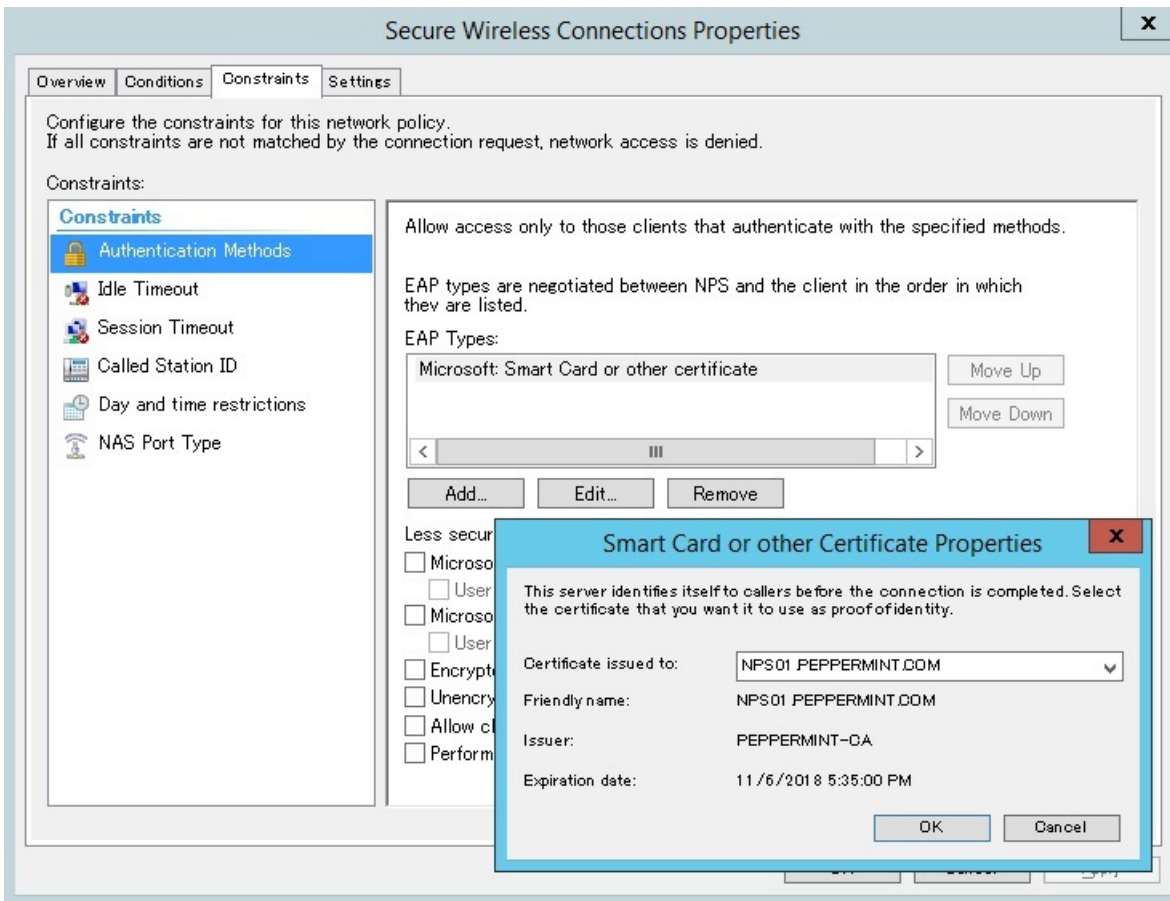


Most 802.1X authentication issues are due to problems with the certificate that is used for client or server authentication (e.g. invalid certificate, expiration, chain verification failure, revocation check failure, etc.).

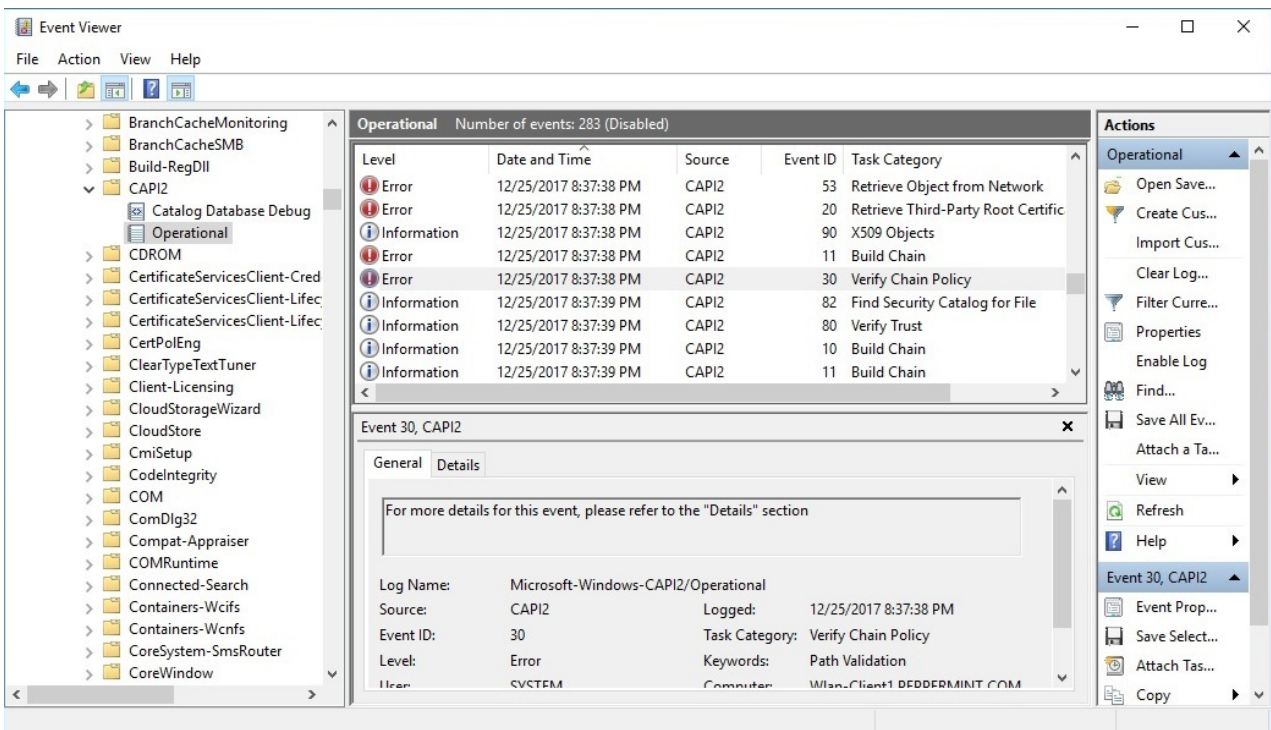
First, validate the type of EAP method being used:

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 if the certificate is valid. For server (NPS) side, you can confirm what certificate is being used from the EAP property menu:

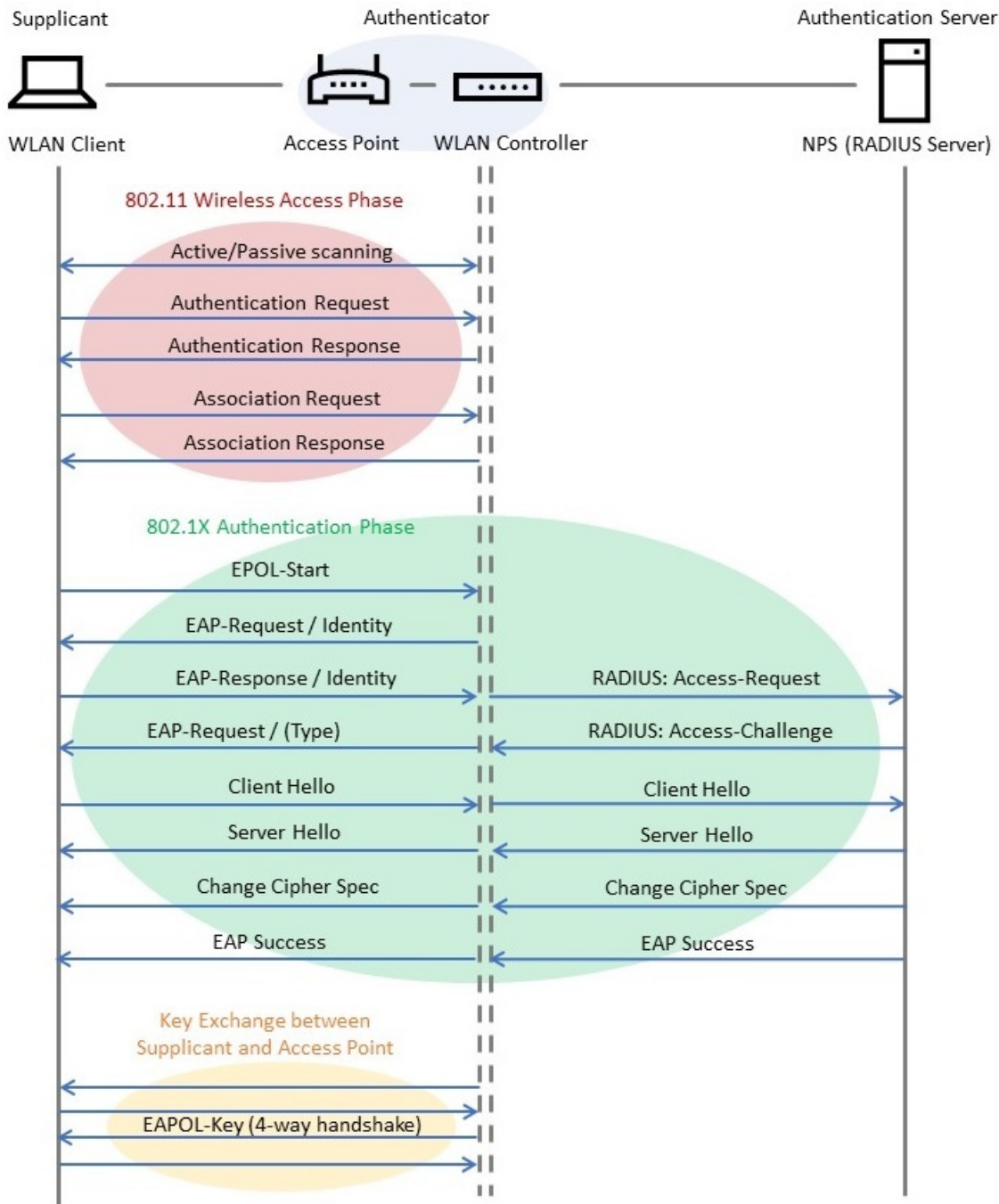


The CAPI2 event log will be useful for troubleshooting certificate-related issues. This log is not enabled by default. You can enable this log by expanding **Event Viewer (Local)\Applications and Services Logs\Microsoft\Windows\CAPI2**, right-clicking **Operational** and then clicking **Enable Log**.



The following article explains how to analyze CAPI2 event logs: [Troubleshooting PKI Problems on Windows Vista](#).

When troubleshooting complex 802.1X authentication issues, it is important to understand the 802.1X authentication process. The following figure is 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 in for a client side capture, and **EAP** for an NPS side capture. See the following examples:

Display Filter: EAPOL

Frame Summary - EAPOL

Frame Number	Time Date Local Adjusted	Protocol Name	Description
76461	14:14:03 2017/12/24	EAP	EAP:Request, Type = Identity
79438	14:14:03 2017/12/24	EAPOL	EAPOL:EAPOL-Start, Length = 0
79714	14:14:03 2017/12/24	EAP	EAP:Request, Type = Identity
80168	14:14:03 2017/12/24	EAP	EAP:Response, Type = Identity
80595	14:14:03 2017/12/24	EAP	EAP:Response, Type = Identity
80620	14:14:03 2017/12/24	EAP	EAP:Request, Type = EAP-TLS
80749	14:14:03 2017/12/24	TLS	TLS:TLS Rec Layer-1 HandShake: Client Hello.
80769	14:14:03 2017/12/24	TLS	TLS:TLS Rec Layer-1 HandShake: Server Hello.; TLS Rec Layer-2 Cipher Change Spec; TLS Rec Layer-3 HandShake: Encrypted Handshake Message.
80885	14:14:03 2017/12/24	TLS	TLS:TLS Rec Layer-1 Cipher Change Spec; TLS Rec Layer-2 HandShake: Encrypted Handshake Message.
80905	14:14:03 2017/12/24	EAP	EAP:Success
81088	14:14:03 2017/12/24	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 1), Length = 117
81926	14:14:03 2017/12/24	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 2), Length = 119
81970	14:14:03 2017/12/24	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 3), Length = 151
81986	14:14:03 2017/12/24	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 4), Length = 95

Client-side packet capture data

Frame ...	Time	Date Local	Adjusted	Protocol...	Source Network...	Source Port	Destination Network...	Destination Port	Description
578	14:14:04	2017/12/24	EAP	10.10.10.100	63637 (0xF895)	10.10.10.30	1812 (0x714)	1812 (0x714)	EAP:Response, Type = Identity
657	14:14:04	2017/12/24	EAP	10.10.10.30	1812 (0x714)	10.10.10.100	63637 (0xF895)	63637 (0xF895)	EAP:Request, Type = EAP-TLS
676	14:14:04	2017/12/24	TLS	10.10.10.100	63637 (0xF895)	10.10.10.30	1812 (0x714)	1812 (0x714)	TLS:TLS Rec Layer-1 Handshake: Client Hello.
702	14:14:04	2017/12/24	TLS	10.10.10.30	1812 (0x714)	10.10.10.100	63637 (0xF895)	63637 (0xF895)	TLS:TLS Rec Layer-1 Handshake: Server Hello.; TLS Rec Layer-2 Cipher Change Spec; TLS Rec Layer-3 Handshake: Encrypted Handshake Message.
708	14:14:04	2017/12/24	TLS	10.10.10.100	63637 (0xF895)	10.10.10.30	1812 (0x714)	1812 (0x714)	TLS:TLS Rec Layer-1 Cipher Change Spec; TLS Rec Layer-2 Handshake: Encrypted Handshake Message.
750	14:14:04	2017/12/24	EAP	10.10.10.30	1812 (0x714)	10.10.10.100	63637 (0xF895)	63637 (0xF895)	EAP:Success

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. Follow the instructions under the **Help** menu in Network Monitor to load the required [parser](#) if needed. See the example below.

The screenshot shows the Microsoft Network Monitor interface. The 'Display Filter' is set to 'WLAN_MicrosoftWindowsWLANAutoConfig'. The main pane shows a list of network events. The selected event (Frame 36817) has the following details:

Frame Number	Time	Date Local	Adjusted	Time Offset	UT	Process Name	Source	Destination	Protocol Name	Description
36817	11:44:11 AM	1/11/2019	9:5674881	(4544)					WLAN_Micro...	WLAN_MicrosoftWindowsWLANAutoConfig:Connection started 1

The 'Hex Details' pane shows the following information:

```

Frame: Number = 36817, Captured Frame Length = 143, MediaType = NetEvent
NetEvent:
MicrosoftWindowsWLANAutoConfig: Connection started 1
  
```

Audit policy

NPS audit policy (event logging) for connection success and failure is enabled by default. 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:

```
auditpol /get /subcategory:"Network Policy Server"
```

If both success and failure events are enabled, the output should be:

System audit policy	
Category/Subcategory	Setting
Logon/Logoff	
Network Policy Server	Success and Failure

If it shows 'No auditing', you can run this command to enable it:

```
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 via Group Policy. The success/failure setting can be found under **Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies -> Logon/Logoff -> Audit Network Policy Server**.

Additional references

[Troubleshooting Windows Vista 802.11 Wireless Connections](#)

[Troubleshooting Windows Vista Secure 802.3 Wired Connections](#)

Data collection for troubleshooting 802.1X authentication

6/6/2019 • 8 minutes to read • [Edit Online](#)

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](#).

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 and Windows 10:

```
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:

```
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

```
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 :

```
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:

```
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

```
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

```
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 :

```
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.

```
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:

```
psr /stop
```

10. Run the following commands from the command prompt on the NPS server.

- To stop RAS trace log and wireless scenario log:

```
netsh trace stop
netsh ras set tracing * disabled
```

- To disable and copy CAPI2 log:

```
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:

```
netsh trace stop
netsh ras set tracing * disabled
```

- To disable and copy the CAPI2 log:

```
wevtutil.exe sl Microsoft-Windows-CAPI2/Operational /e:false
wevtutil.exe ep1 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

```
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

```
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:

```
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:


```

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%_cert-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:

```

netsh wlan show all > c:\MSLOG\%COMPUTERNAME%_wlan_show_all.txt
netsh wlan export profile folder=c:\MSLOG\

```

- Wired LAN Client information

```

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:

```
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:

```
wevtutil ep1 Application c:\MSLOG\%COMPUTERNAME%\Application.evtx
wevtutil ep1 System c:\MSLOG\%COMPUTERNAME%\System.evtx
wevtutil ep1 Security c:\MSLOG\%COMPUTERNAME%\Security.evtx
wevtutil ep1 Microsoft-Windows-GroupPolicy/Operational
c:\MSLOG\%COMPUTERNAME%\GroupPolicy_Operational.evtx
wevtutil ep1 Microsoft-Windows-CertificateServicesClient-CredentialRoaming/Operational
c:\MSLOG\%COMPUTERNAME%\CertificateServicesClient-CredentialRoaming_Operational.evtx
wevtutil ep1 Microsoft-Windows-CertPoleEng/Operational
c:\MSLOG\%COMPUTERNAME%\CertPoleEng_Operational.evtx
```

- Run the following 3 commands on Windows Server 2012 and later:

```
wevtutil ep1 Microsoft-Windows-CertificateServicesClient-Lifecycle-System/Operational
c:\MSLOG\%COMPUTERNAME%\CertificateServicesClient-Lifecycle-System_Operational.evtx
wevtutil ep1 Microsoft-Windows-CertificateServicesClient-Lifecycle-User/Operational
c:\MSLOG\%COMPUTERNAME%\CertificateServicesClient-Lifecycle-User_Operational.evtx
wevtutil ep1 Microsoft-Windows-CertificateServices-Deployment/Operational
c:\MSLOG\%COMPUTERNAME%\CertificateServices-Deployment_Operational.evtx
```

- Certificates store information

```

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%_cert-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:

```

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. Click **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

```
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

```
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 3 lines on Windows 2012 and up

```
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

```

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%_cert-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

```

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. Log on 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.

```
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 for TCP/IP issues

5/31/2019 • 2 minutes to read • [Edit Online](#)

In these topics, you will learn how to troubleshoot common problems in a TCP/IP network environment.

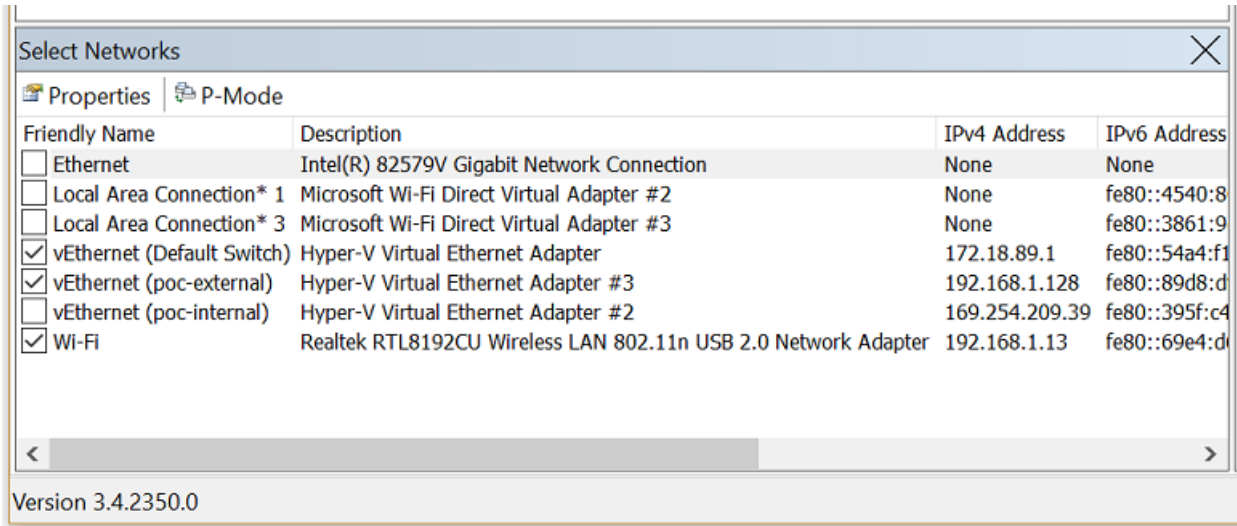
- [Collect data using Network Monitor](#)
- [Troubleshoot TCP/IP connectivity](#)
- [Troubleshoot port exhaustion issues](#)
- [Troubleshoot Remote Procedure Call \(RPC\) errors](#)

Collect data using Network Monitor

5/31/2019 • 2 minutes to read • [Edit Online](#)

In this topic, you will learn how to use Microsoft Network Monitor 3.4, which is a tool for capturing network traffic.

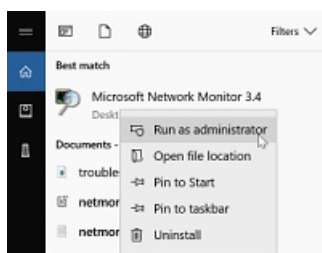
To get started, [download and run NM34_x64.exe](#). When you install Network Monitor, it installs its driver and hooks it to all the network adapters installed on the device. You can see the same on the adapter properties, as shown in the following image.



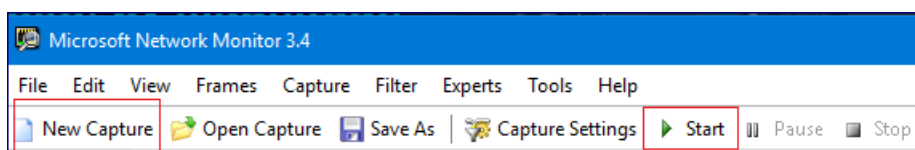
When the driver gets hooked to the network interface card (NIC) during installation, the NIC is reinitialized, which might cause a brief network glitch.

To capture traffic

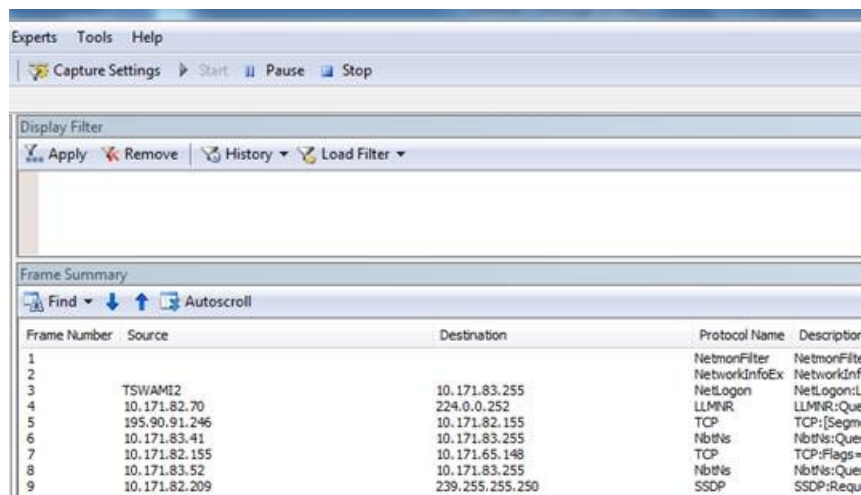
1. Run netmon in an elevated status by choosing Run as Administrator.



2. Network Monitor opens with all network adapters displayed. Select the network adapters where you want to capture traffic, click **New Capture**, and then click **Start**.



3. Reproduce the issue, and you will 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 are facing. So you will 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.tcpretransmits
- 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 which 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](#)

Troubleshoot TCP/IP connectivity

5/31/2019 • 5 minutes to read • [Edit Online](#)

You might come across connectivity errors on the application end or timeout errors. Most common scenarios would include application connectivity to a database server, SQL timeout errors, BizTalk application timeout errors, Remote Desktop Protocol (RDP) failures, file share access failures, or 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 which could indicate a network issue.

- TCP is defined as connection-oriented and reliable protocol. One of the ways in which TCP ensures this is through the handshake process. Establishing a TCP session would begin with a 3-way handshake, followed by data transfer, and then a 4-way closure. The 4-way closure where both sender and receiver agree on closing the session is termed as *graceful closure*. After the 4-way closure, the server will allow 4 minutes of time (default), during which any pending packets on the network are to be processed, this is the TIME_WAIT state. Once the TIME_WAIT state is done, all the resources allocated for this connection are released.
- TCP reset is an abrupt closure of the session which 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 which will help you 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 will see a RESET.

Packet drops

When one TCP peer is sending out TCP packets for which there is no response received from the other end, the TCP peer would end up re-transmitting the data and when there is no response received, it would end the session by sending an ACK RESET (meaning, application acknowledges whatever data exchanged so far, but due to packet drop closing the connection).

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 would mean, 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 3 times.

Source side connecting on port 445:

Apply Remove History Load Filter

ipv4.Address==10.10.10.1 and ipv4.Address==10.10.10.2

Frame Summary - tcp.port==445

Find Autoscroll

Source	Destination	Protocol Name	Description
10.10.10.1	10.10.10.2	TCP	TCP:Flags=CE...S., SrcPort=59110, DstPort=Microsoft-DS(445), PayloadLen=0, Seq=93
10.10.10.1	10.10.10.2	TCP	TCP:[SynRetransmit #3]Flags=CE...S., SrcPort=59110, DstPort=Microsoft-DS(445), Pay
10.10.10.1	10.10.10.2	TCP	TCP:[SynRetransmit #3]Flags=...S., SrcPort=59110, DstPort=Microsoft-DS(445), Payc

Destination side: applying the same filter, you do not see any packets.

Apply Remove History Load Filter

ipv4.Address==10.10.10.1 and ipv4.Address==10.10.10.2

Frame Summary - ipv4.Address==10.10.10.1 and ipv4.Address==10.10.10.2

Find Autoscroll

Source	Destination	Protocol Name	Description
--------	-------------	---------------	-------------

For the rest of the data, TCP will retransmit the packets 5 times.

Source 192.168.1.62 side trace:

192.168.1.62	192.168.1.2	SMB2	SMB2:C CREATE (0x5), Sh(RWD), DhnQ+MxAc, File=NULL@#559
192.168.1.62	192.168.1.2	TCP	TCP:[Retransmit #554]Flags=...AP..., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=536, Seq=815994039 - 815994
192.168.1.62	192.168.1.2	TCP	TCP:[Retransmit #554]Flags=...AP..., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=536, Seq=815994039 - 815994
192.168.1.62	192.168.1.2	TCP	TCP:[Retransmit #554]Flags=...AP..., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=756, Seq=815994039 - 815994
192.168.1.62	192.168.1.2	TCP	TCP:[Retransmit #554]Flags=...AP..., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=756, Seq=815994039 - 815994
192.168.1.62	192.168.1.2	TCP	TCP:[Retransmit #554]Flags=...AP..., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=756, Seq=815994039 - 815994
192.168.1.62	192.168.1.2	TCP	TCP:Flags=...A.R., SrcPort=51457, DstPort=Microsoft-DS(445), PayloadLen=0, Seq=815994795, Ack=4172207889, Win=0 (sci

Destination 192.168.1.2 side trace:

You would not 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 are seeing that the SYN packets are reaching the destination, but the destination is still not responding, then verify if the port that you are trying to connect to is in the listening state. (Netstat output will help). If the port is listening and still there is 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 re-played 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 will be able to notice if there is a change in the packets itself or if any new packets are reaching the destination on behalf of the source.

In this case, you will again need help from the network team to identify any such device which is modifying packets or re-playing packets to the destination. The most common ones are RiverBed devices or WAN accelerators.

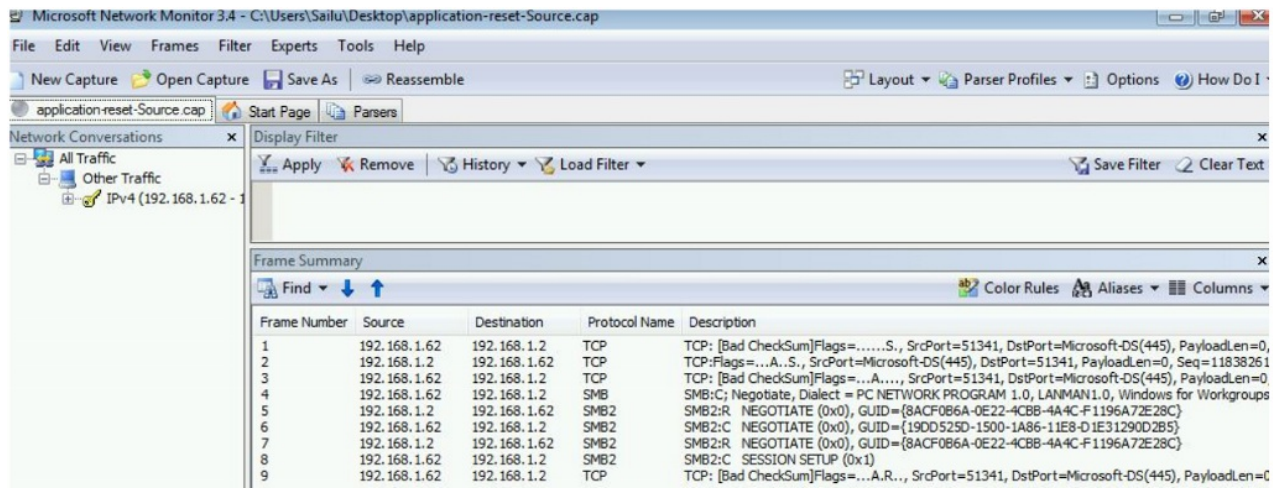
Application side reset

When you have identified that the resets are not due to retransmits or incorrect parameter or packets being modified with the help of network trace, then you have narrowed it down to application level reset.

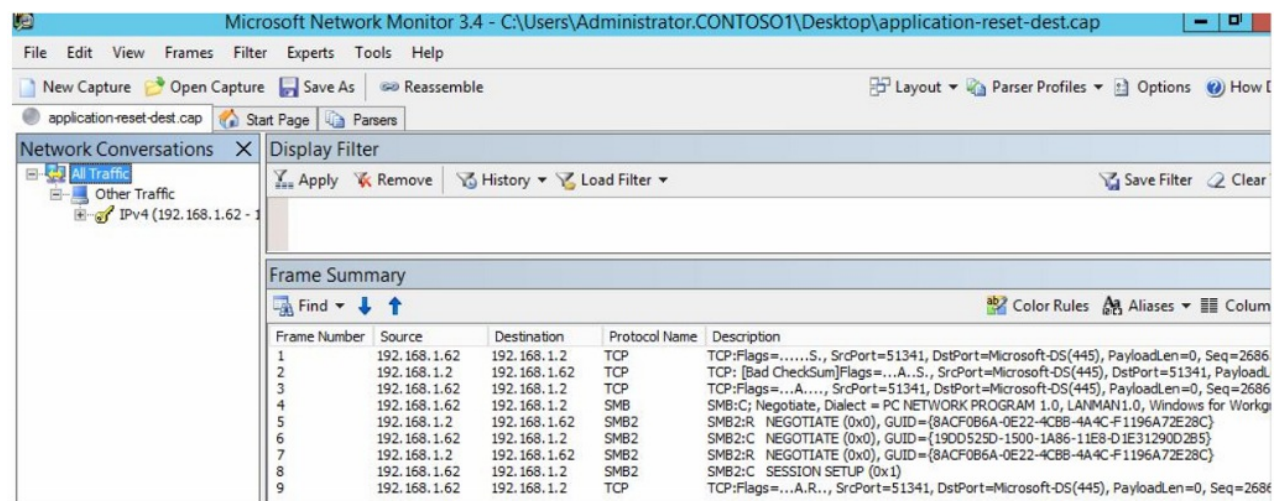
The application resets are the ones where you see the Acknowledgement flag set to **1** along with the reset flag. This would mean that the server is acknowledging the receipt of the packet but for some reason it will not accept the connection. This is when the application that received the packet did not 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 does not 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 which is 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 would not see retransmission or resets when using UDP as a transport protocol. However, UDP makes use of ICMP as an error reporting protocol. When you have the UDP packet sent out on a port and the destination does not have port listed, you will see the destination sending out **ICMP Destination host unreachable: Port unreachable** message immediately after the UDP packet

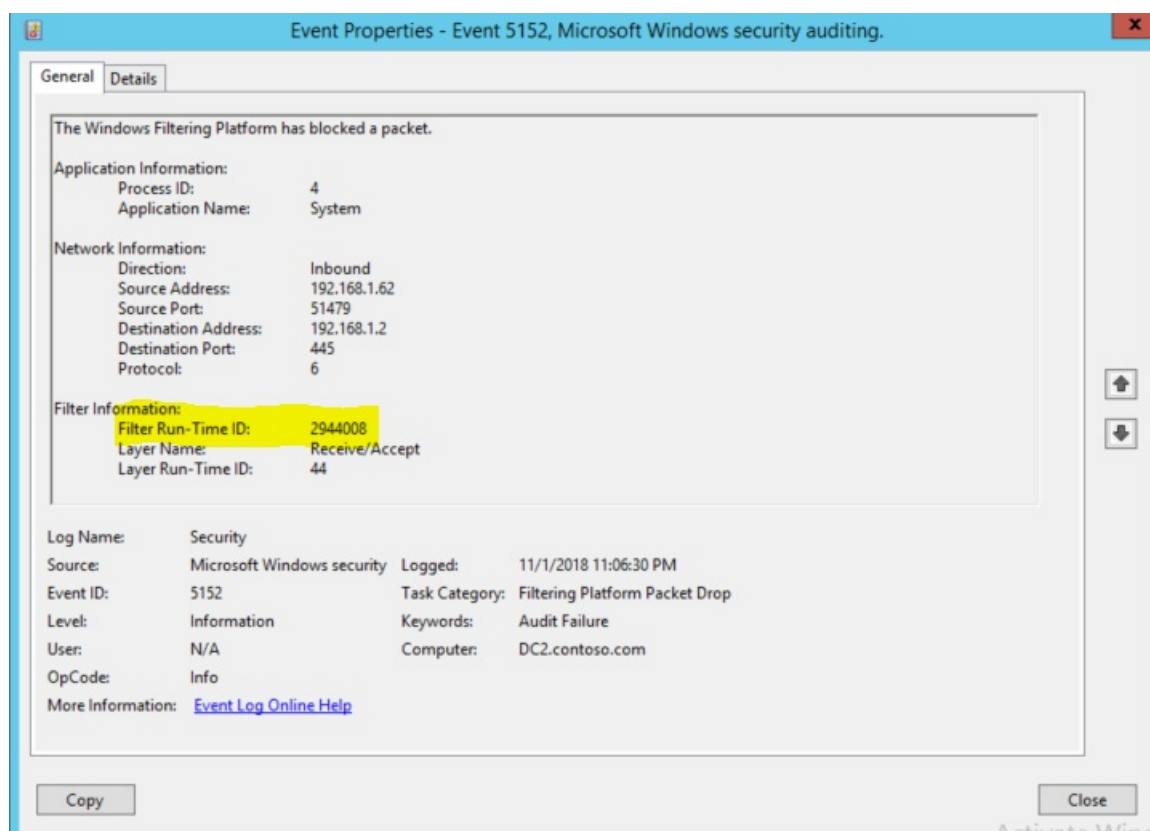
```
10.10.10.1 10.10.10.2 UDP UDP:SrcPort=49875,DstPort=3343
```

```
10.10.10.2 10.10.10.1 ICMP ICMP:Destination Unreachable Message, Port Unreachable,10.10.10.2:3343
```

During the course of troubleshooting connectivity issue, you might also see in the network trace that a machine receives packets but does not respond to. In such cases, there could be a drop at the server level. You should enable firewall auditing on the machine to understand if the local firewall is dropping the packet.

```
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 will generate a wfpstate.xml file. Once you open this file and filter for the ID you find in the above event (2944008), you will be able to see a firewall rule name associated with this ID which is blocking the connection.


```
        <uint64>274877906944</uint64>
    </effectiveWeight>
</item>
<item>
    <displayData>
        <name>tcp port 445</name>
        <description/>
    </displayData>

    <action>
        <type>FWP_ACTION_BLOCK</type>
        <filterType/>
    </action>
    <rawContext>0</rawContext>
    <reserved/>
    <filterId>2944008</filterId>
    <effectiveWeight>
        <type>FWP_UINT64</type>
        <uint64>11531326108393799680</uint64>
    </effectiveWeight>
</item>
<item>
```

Troubleshoot port exhaustion issues

6/6/2019 • 9 minutes to read • [Edit Online](#)

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 usually 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.

Clients when connecting to an application or service will make use of an ephemeral port from its machine 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 a lot of connections to multiple website, for any new connection that the browser is attempting, an ephemeral port is used. After some time, you will notice that the connections will start to fail and one high possibility for this 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 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:

- `netsh int ipv4 show dynamicport tcp`
- `netsh int ipv4 show dynamicport udp`
- `netsh int ipv6 show dynamicport tcp`
- `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.

```
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:

- `netsh int ipv4 set dynamicport tcp start=10000 num=1000`

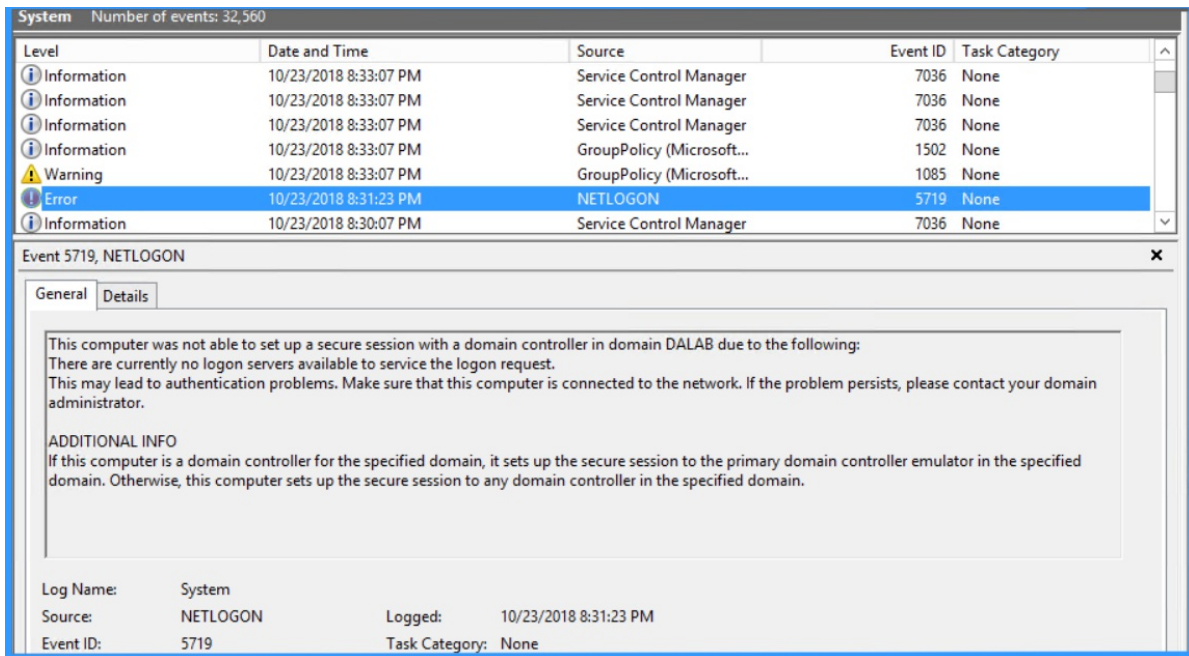
- `netsh int ipv4 set dynamicport udp start=10000 num=1000`
- `netsh int ipv6 set dynamicport tcp start=10000 num=1000`
- `netsh int ipv6 set dynamicport udp start=10000 num=1000`

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) cannot 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 results in a start port of 1025 and an end port of 5000.

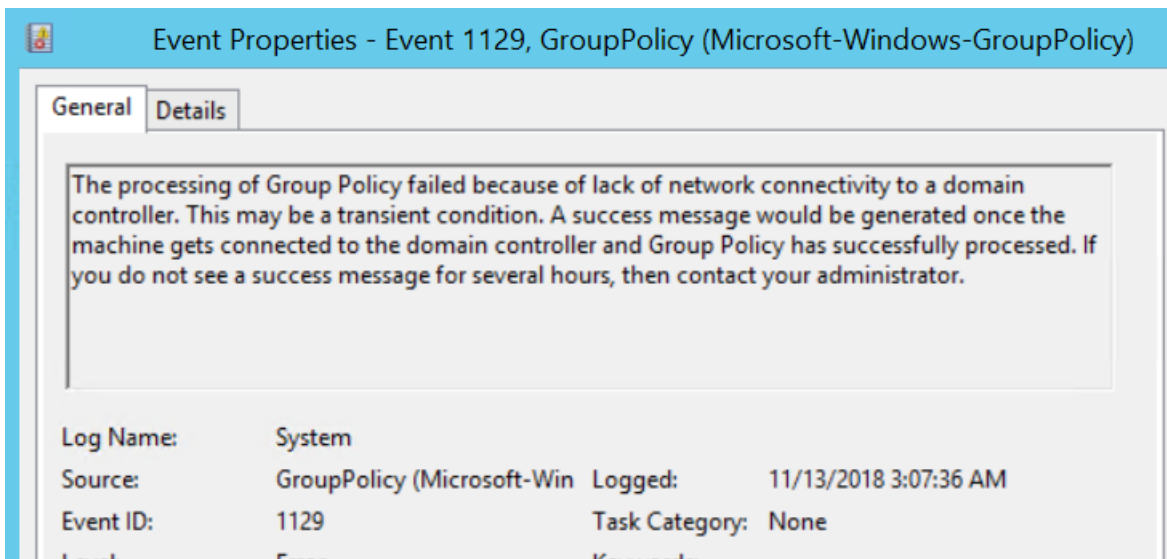
Specifically, about outbound connections as incoming connections will not require an Ephemeral port for accepting connections.

Since outbound connections start to fail, you will see a lot of the below behaviors:

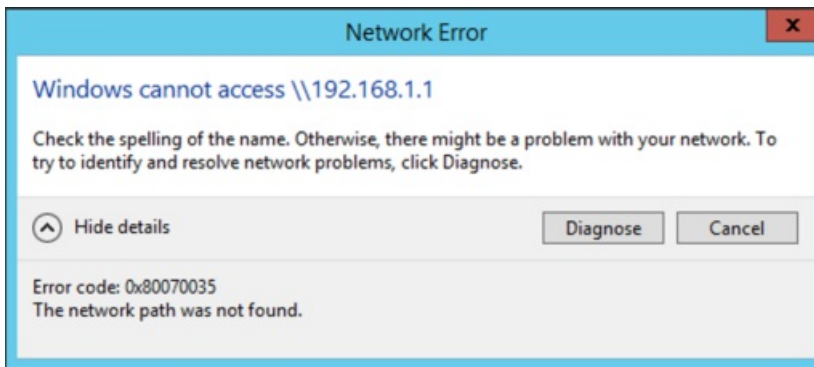
- Unable to sign in to the machine with domain credentials, however sign-in with local account works. Domain sign-in will require you to contact the DC for authentication which is again an outbound connection. If you have cache credentials set, then domain sign-in might still work.



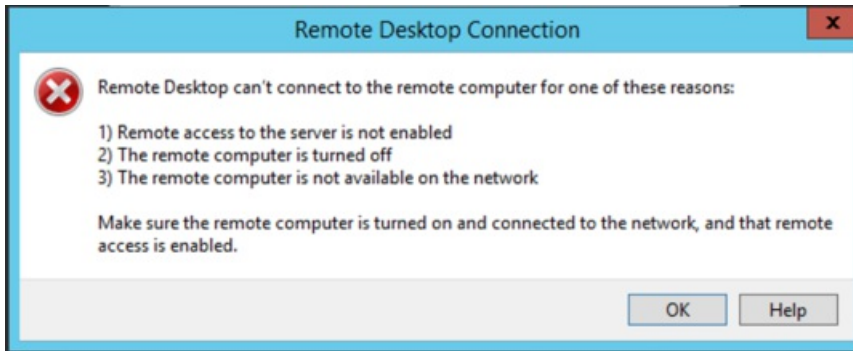
- Group Policy update failures:



- 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, go to the next step.
2. Open event viewer and under the system logs, look for the events which clearly indicate the current state:

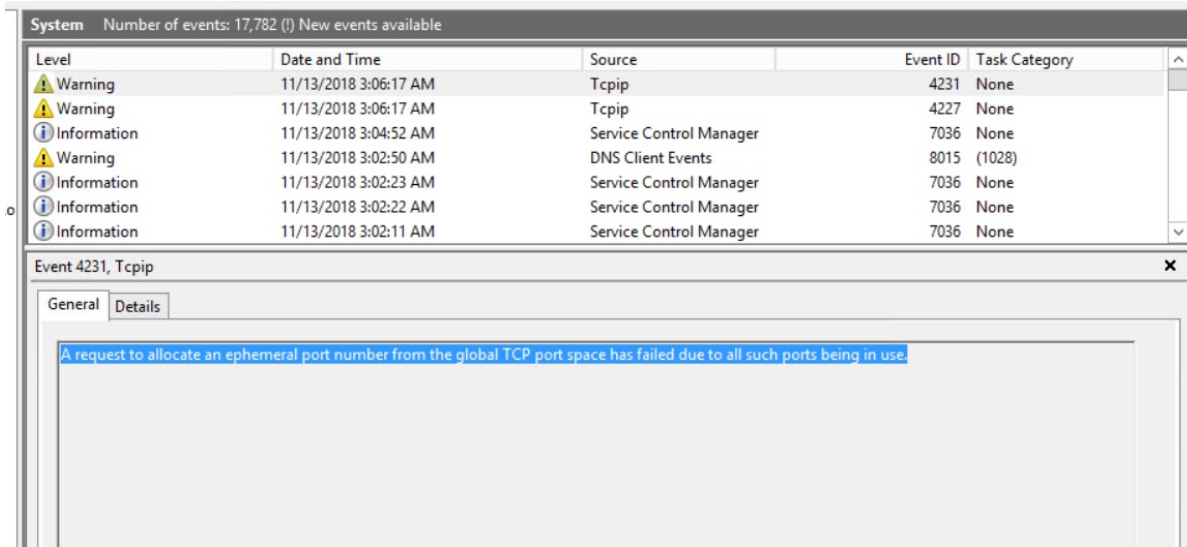
a. Event ID 4227

Level	Date and Time	Source	Event ID	Task Category
Warning	11/13/2018 3:06:17 AM	Tcpip	4231	None
Warning	11/13/2018 3:06:17 AM	Tcpip	4227	None
Information	11/13/2018 3:04:52 AM	Service Control Manager	7036	None
Warning	11/13/2018 3:02:50 AM	DNS Client Events	8015 (1028)	
Information	11/13/2018 3:02:23 AM	Service Control Manager	7036	None
Information	11/13/2018 3:02:22 AM	Service Control Manager	7036	None
Information	11/13/2018 3:02:11 AM	Service Control Manager	7036	None

Event 4227, Tcpip

General		Details	
<p>TCP/IP failed to establish an outgoing connection because the selected local endpoint was recently used to connect to the same remote endpoint. This error typically occurs when outgoing connections are opened and closed at a high rate, causing all available local ports to be used and forcing TCP/IP to reuse a local port for an outgoing connection. To minimize the risk of data corruption, the TCP/IP standard requires a minimum time period to elapse between successive connections from a given local endpoint to a given remote endpoint.</p>			
Log Name:	System	Logged:	11/13/2018 3:06:17 AM
Source:	Tcpip	Task Category:	None
Event ID:	4227		

b. Event ID 4231



- 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 40.77.226.250:443 TIME_WAIT 1243
TCP 10.94.160.76:53401 104.211.216.33:443 TIME_WAIT 1243
TCP 10.94.160.76:53402 13.76.141.123:443 TIME_WAIT 1243
TCP 10.94.160.76:53403 13.76.141.123:443 TIME_WAIT 1243
TCP 10.94.160.76:53404 117.18.232.200:443 TIME_WAIT 1243
TCP 10.94.160.76:53406 65.55.44.109:443 TIME_WAIT 1243
TCP 10.94.160.76:53407 65.55.44.109:443 TIME_WAIT 1243
TCP 10.94.160.76:53408 13.76.142.215:443 TIME_WAIT 1243
TCP 10.94.160.76:53409 13.76.142.215:443 TIME_WAIT 1243
TCP 10.94.160.76:53410 40.81.31.55:443 TIME_WAIT 1243
TCP 10.94.160.76:53411 40.81.31.55:443 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 52.109.124.5:443 TIME_WAIT 1243
TCP 10.94.160.76:53446 52.109.124.5:443 TIME_WAIT 1243
TCP 10.94.160.76:53448 10.151.148.80:80 TIME_WAIT 1243
TCP 10.94.160.76:53460 52.114.128.8:443 TIME_WAIT 1243
TCP 10.94.160.76:53463 52.114.76.37:443 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 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 will not be able to release all the ports that it has consumed and will remain in the TIME_WAIT state.

You may 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 does not necessarily indicate port exhaustion.

NOTE

Having huge connections in TIME_WAIT state does not 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

```
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 which say **STATUS_TOO_MANY_ADDRESSES**. If you do not 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 are using Windows 10 or Windows Server 2016, then you can run the command `netstat -anobq` and check for the process ID which has maximum entries as BOUND. Alternately, you can also run the below Powershell command to identify the process:

```
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
```

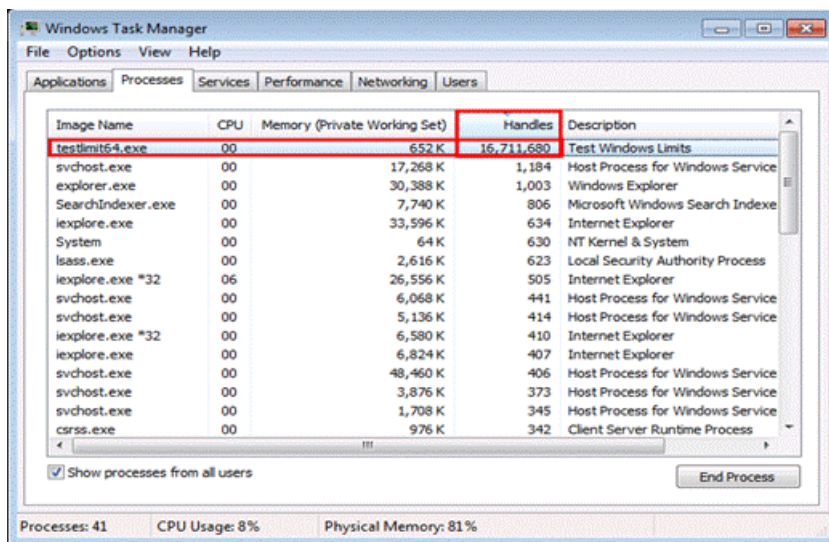
Most port leaks are caused by user-mode processes not correctly closing the ports when an error was encountered. At the user-mode level ports (actually sockets) are handles. Both **TaskManager** and **ProcessExplorer** are able to display handle counts which allows you to identify which process is consuming 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 does not 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 has a higher number, stop that process and then try to login using domain credentials and see if it succeeds.

Method 3

If Task Manager did not 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 + click 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. Click 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


```
@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
```

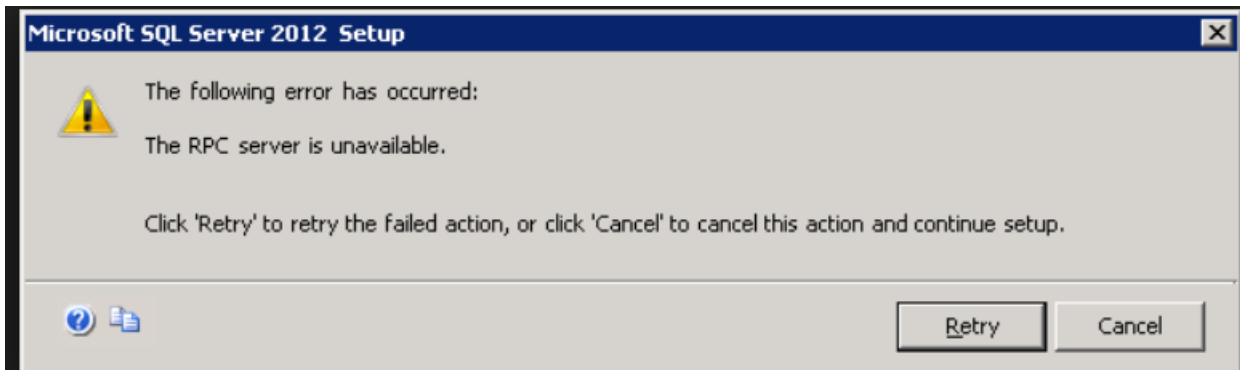
Useful links

- [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 which will run in a loop to report the port status. (Applicable for Windows 2012 R2, Windows 8, Windows 10)

Troubleshoot Remote Procedure Call (RPC) errors

6/26/2019 • 7 minutes to read • [Edit Online](#)

You might encounter an **RPC server unavailable** error when connecting to Windows Management Instrumentation (WMI), SQL Server, during a remote connection, or for some Microsoft Management Console (MMC) snap-ins. The following image is an example of an RPC error.



This is a commonly encountered error message in the networking world and one can lose hope very fast without trying to understand much, as to what is happening 'under the hood'.

Before getting in to troubleshooting the **RPC server unavailable-* error, let's first understand basics about the error. There are a few important terms to understand:

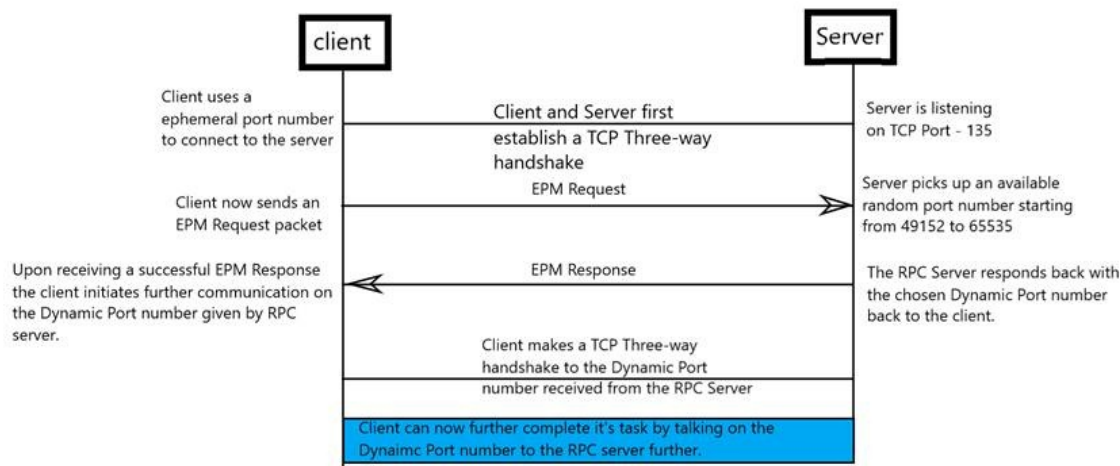
- Endpoint mapper – a service listening on the server, which guides client apps to server apps by port and UUID.
- Tower – describes the RPC protocol, to allow the client and server to negotiate a connection.
- Floor – the contents of a tower with specific data like ports, IP addresses, and identifiers.
- UUID – a well-known GUID that identifies the RPC application. The UUID is what you use to see a specific kind of RPC application conversation, as there are likely to be many.
- Opnum – the identifier of a function that the client wants the server to execute. It's just a hexadecimal number, but a good network analyzer will translate the function for you. If neither knows, your application vendor must tell you.
- Port – the communication endpoints for the client and server applications.
- Stub data – the information given to functions and data exchanged between the client and server. This is the payload, the important part.

NOTE

A lot of the above information is used in troubleshooting, the most important is the Dynamic RPC port number you get while talking to EPM.

How the connection works

Client A wants to execute some functions or wants to make use of a service running on the remote server, will first establish the connection with the Remote Server by doing a three-way handshake.



RPC ports can be given from a specific range as well.

Configure RPC dynamic port allocation

Remote Procedure Call (RPC) dynamic port allocation is used by server applications and remote administration applications such as Dynamic Host Configuration Protocol (DHCP) Manager, Windows Internet Name Service (WINS) Manager, and so on. RPC dynamic port allocation will instruct the RPC program to use a particular random port in the range configured for TCP and UDP, based on the implementation of the operating system used.

Customers using firewalls may want to control which ports RPC is using so that their firewall router can be configured to forward only these Transmission Control Protocol (UDP and TCP) ports. Many RPC servers in Windows let you specify the server port in custom configuration items such as registry entries. When you can specify a dedicated server port, you know what traffic flows between the hosts across the firewall, and you can define what traffic is allowed in a more directed manner.

As a server port, please choose a port outside of the range you may want to specify below. You can find a comprehensive list of server ports that are used in Windows and major Microsoft products in the article [Service overview and network port requirements for Windows](#). The article also lists the RPC servers and which RPC servers can be configured to use custom server ports beyond the facilities the RPC runtime offers.

Some firewalls also allow for UUID filtering where it learns from a RPC Endpoint Mapper request for a RPC interface UUID. The response has the server port number, and a subsequent RPC Bind on this port is then allowed to pass.

With Registry Editor, you can modify the following parameters for RPC. The RPC Port key values discussed below are all located in the following key in the registry:

HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\Internet\ Entry name Data Type

Ports REG_MULTI_SZ

- Specifies a set of IP port ranges consisting of either all the ports available from the Internet or all the ports not available from the Internet. Each string represents a single port or an inclusive set of ports. For example, a single port may be represented by **5984**, and a set of ports may be represented by **5000-5100**. If any entries are outside the range of 0 to 65535, or if any string cannot be interpreted, the RPC runtime treats the entire configuration as invalid.

PortsInternetAvailable REG_SZ Y or N (not case-sensitive)

- If Y, the ports listed in the Ports key are all the Internet-available ports on that computer. If N, the ports listed in the Ports key are all those ports that are not Internet-available.

UseInternetPorts REG_SZ) Y or N (not case-sensitive)

- Specifies the system default policy.
- If Y, the processes using the default will be assigned ports from the set of Internet-available ports, as defined previously.
- If N, the processes using the default will be assigned ports from the set of intranet-only ports.

Example:

In this example ports 5000 through 6000 inclusive have been arbitrarily selected to help illustrate how the new registry key can be configured. This is not a recommendation of a minimum number of ports needed for any particular system.

1. Add the Internet key under: HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc
2. Under the Internet key, add the values "Ports" (MULTI_SZ), "PortsInternetAvailable" (REG_SZ), and "UseInternetPorts" (REG_SZ).

For example, the new registry key appears as follows: Ports: REG_MULTI_SZ: 5000-6000
PortsInternetAvailable: REG_SZ: Y UseInternetPorts: REG_SZ: Y

3. Restart the server. All applications that use RPC dynamic port allocation use ports 5000 through 6000, inclusive.

You should open up a range of ports above port 5000. Port numbers below 5000 may already be in use by other applications and could cause conflicts with your DCOM application(s). Furthermore, previous experience shows that a minimum of 100 ports should be opened, because several system services rely on these RPC ports to communicate with each other.

NOTE

The minimum number of ports required may differ from computer to computer. Computers with higher traffic may run into a port exhaustion situation if the RPC dynamic ports are restricted. Take this into consideration when restricting the port range.

WARNING

If there is an error in the port configuration or there are insufficient ports in the pool, the Endpoint Mapper Service will not be able to register RPC servers with dynamic endpoints. When there is a configuration error, the error code will be 87 (0x57) ERROR_INVALID_PARAMETER. This can affect Windows RPC servers as well, such as Netlogon. It will log event 5820 in this case:

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.'

If you would like to do a deep dive as to how it works, see [RPC over IT/Pro](#).

Troubleshooting RPC error

PortQuery

The best thing to always troubleshoot RPC issues before even getting in to traces is by making use of tools like **PortQry**. You can quickly determine if you are able to make a connection by running the command:

```
Portqry.exe -n <ServerIP> -e 135
```

This would give you a lot of output to look for, but you should be looking for **ip_tcp-* and the port number in the

brackets, which tells whether you were successfully able to get a dynamic port from EPM and also make a connection to it. If the above fails, you can typically start collecting simultaneous network traces. Something like this from the output of "PortQry":

```
Portqry.exe -n 169.254.0.2 -e 135
```

Partial output below:

```
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 ncaen_ip_tcp:169.254.0.10[49664]
```

The one in bold is the ephemeral port number that you made a connection to successfully.

Netsh

You can run the commands below to leverage Windows inbuilt netsh captures, to collect a simultaneous trace. Remember to execute the below on an "Admin CMD", it requires elevation.

- On the client

```
Netsh trace start scenario=netconnection capture=yes tracefile=c:\client_nettrace.etl maxsize=512  
overwrite=yes report=yes
```

- On the Server

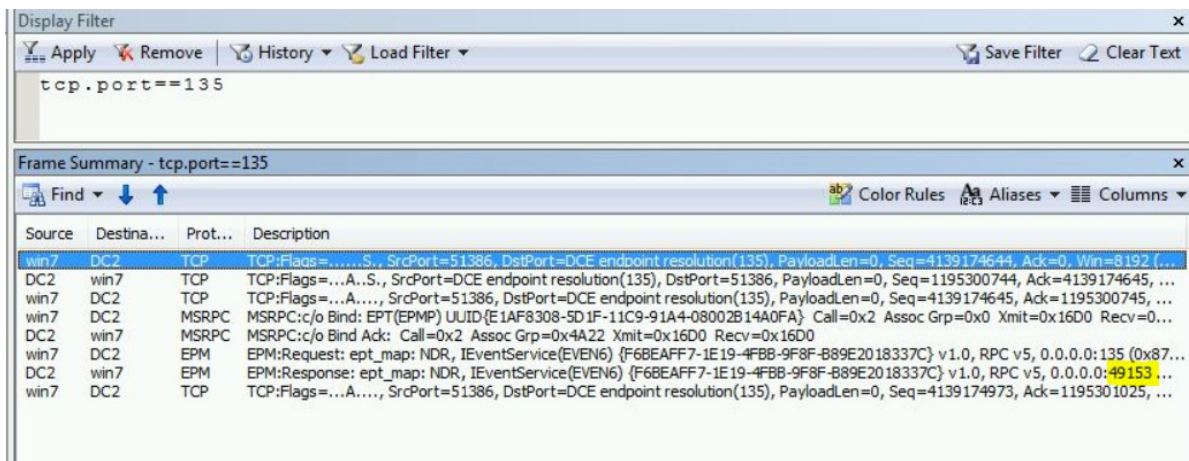
```
Netsh trace start scenario=netconnection capture=yes tracefile=c:\server_nettrace.etl maxsize=512  
overwrite=yes report=yes
```

Now try to reproduce your issue from the client machine and as soon as you feel the issue has been reproduced, go ahead and stop the traces using the command

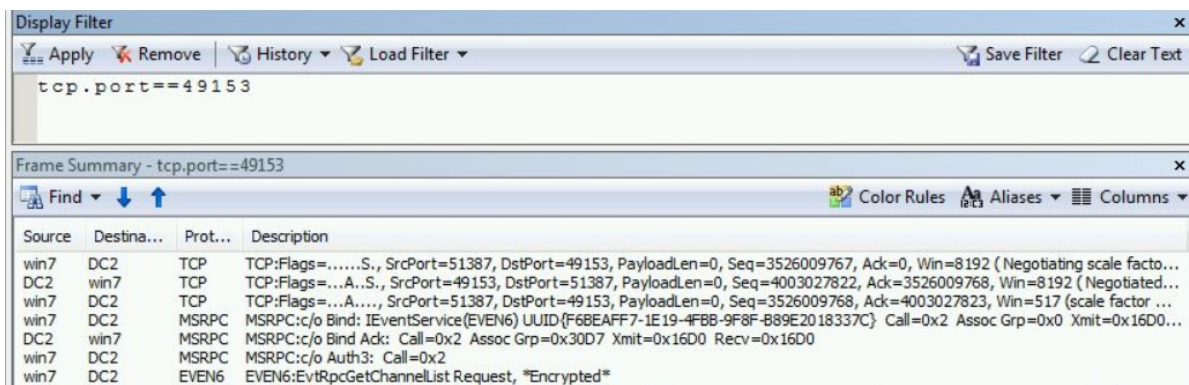
```
Netsh trace stop
```

Open the traces in [Microsoft Network Monitor 3.4](#) or Message Analyzer and filter the trace for

- `Ipv4.address==<client-ip>` and `ipv4.address==<server-ip>` and `tcp.port==135` or just `tcp.port==135` should help.
- Look for the "EPM" Protocol Under the "Protocol" column.
- Now check if you are getting a response from the server. If you get a response, note the dynamic port number that you have been allocated to use.



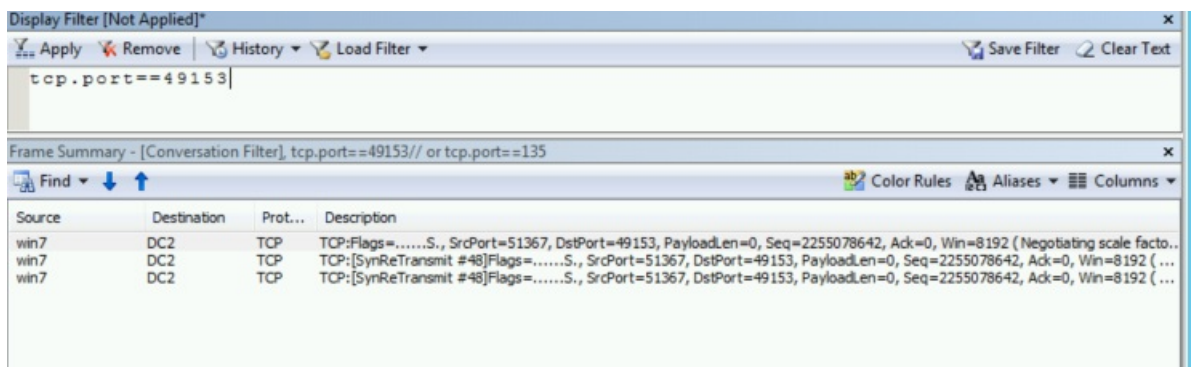
- Check if we are connecting successfully to this Dynamic port successfully.
- The filter should be something like this: `tcp.port==<dynamic-port-allocated>` and `ipv4.address==<server-ip>`



This should help you verify the connectivity and isolate if any network issues are seen.

Port not reachable

The most common reason why we would see the RPC server unavailable is when the dynamic port that the client tries to connect is not reachable. The client side trace would then show TCP SYN retransmits for the dynamic port.



The port cannot be reachable due to one of the following reasons:

- 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 (WFP drop / NIC drop/ Filter driver etc).

Advanced troubleshooting for Windows start-up issues

5/31/2019 • 2 minutes to read • [Edit Online](#)

In these topics, you will learn how to troubleshoot common problems related to Windows start-up.

- [Advanced troubleshooting for Windows boot problems](#)
- [Advanced troubleshooting for Stop error or blue screen error](#)
- [Advanced troubleshooting for Windows-based computer freeze issues](#)

Advanced troubleshooting for Windows boot problems

6/6/2019 • 11 minutes to read • [Edit Online](#)

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](#).

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 additional 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 are not marked BOOT_START.

Here is a summary of the boot sequence, what will be seen on the display, and typical boot problems at that point in the sequence. Before starting 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.



[Click to enlarge](#)

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 is not working, this 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 does not, this 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 completely black except for a blinking cursor, or if you receive one of the following error codes, this 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, follow these steps.

NOTE

For additional methods to start WinRE, see [Entry points into WinRE](#).

1. Start the system to the installation media for the installed version of Windows.

Note For more information, see [Create installation media for Windows](#).

2. On the **Install Windows** screen, select **Next > Repair your computer**.

3. On the **System Recovery Options** screen, select **Next > Command Prompt**.

4. 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\Srtrtail.txt

For more information see, [A Stop error occurs, or the computer stops responding when you try to start Windows Vista or Windows 7](#)

Method 2: Repair Boot Codes

To repair boot codes, run the following command:

```
BOOTREC /FIXMBR
```

To repair the boot sector, run the following command:

```
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, run the following command:

```
Bootrec /ScanOS
```

2. Restart the computer to check whether the problem is fixed.

3. If the problem is not fixed, run the following command:

```
Bootrec /rebuildbcd
```

4. You might receive one of the following outputs:

- Scanning all disks for Windows installations. Please wait, since this may take a while...Successfully scanned Windows installations. Total identified Windows installations: 0 The operation completed successfully.

- Scanning all disks for Windows installations. Please wait, since this may take a while... Successfully scanned Windows installations. Total identified Windows installations: 1 D:\Windows
Add installation to boot list? Yes/No/All:

If the output shows **windows installation: 0**, run the following commands:

```
bcdedit /export c:\bcdbackup  
  
attrib c:\boot\bcd -h -r -s  
  
ren c:\boot\bcd bcd.old  
  
bootrec /rebuildbcd
```

After you run the command, you receive the following output:

```
Scanning all disks for Windows installations. Please wait, since this may take a while...Successfully scanned  
Windows installations. Total identified Windows installations: 1{D}:\Windows
```

Add installation to boot list? Yes/No/All: Y

5. Try again to start the system.

Method 4: Replace Bootmgr

If methods 1 and 2 do not fix the problem, replace the Bootmgr file from drive C to the System Reserved partition. To do this, 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:

```
attrib -s -h -r
```

3. Run the same **attrib** command on the Windows (system drive):

```
attrib -s -h -r
```

4. Rename the Bootmgr file as Bootmgr.old:

```
ren c:\bootmgr bootmgr.old
```

5. Start a text editor, such as Notepad.
6. Navigate to the system drive.
7. Copy the Bootmgr file, and then paste it to the System Reserved partition.
8. Restart the computer.

Method 5: Restore System Hive

If Windows cannot load the system registry hive into memory, you must restore the system hive. To do this, use the Windows Recovery Environment or use Emergency Repair Disk (ERD) to copy the files from the C:\Windows\System32\config\RegBack 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.

Kernel Phase

If the system gets stuck during the kernel phase, you experience multiple symptoms or receive multiple error messages. These include, but are not limited to, the following:

- A Stop error appears after the splash screen (Windows Logo screen).
- Specific error code is displayed. For example, "0x00000C2" , "0x0000007B" , "inaccessible boot device" and so on. (To troubleshoot the 0x0000007B error, see [Error code INACCESSIBLE_BOOT_DEVICE \(STOP 0x7B\)](#))
- 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:
 - Click **Start**, point to **Administrative Tools**, and then click **Event Viewer**.
 - Start the Event Viewer snap-in in Microsoft Management Console (MMC).
2. In the console tree, expand Event Viewer, and then click the log that you want to view. For example, click **System log** or **Application log**.
3. In the details pane, double-click the event that you want to view.
4. On the **Edit** menu, click **Copy**, open a new document in the program in which you want to paste the event (for example, Microsoft Word), and then click **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 cannot 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 cannot 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 same version of Windows or a later version.
2. Open the registry.
3. Load the system hive, and name it as "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, click the upper or lower filter, and then delete the value data.
6. Search through the whole registry for similar items. Process as an appropriate, and then unload the registry hive.
7. Restart the server in Normal mode.

For additional troubleshooting steps, see the following articles:

- [Troubleshooting a Stop 0x7B in Windows](#)
- [Advanced troubleshooting for "Stop error code 0x0000007B \(INACCESSIBLE_BOOT_DEVICE\)" errors in Windows XP.](#)

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:

```
dism /image:C:\ /get-packages
```

3. If there are any pending updates, uninstall them by running the following commands:

```
DISM /image:C:\ /remove-package /packagename: name of the package
```

```
Dism /Image:C:\ /Cleanup-Image /RevertPendingActions
```

Try to start the computer.

If the computer does not 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 a test.
5. Highlight the loaded test hive, and then search for the **pendingxmlidentifier** value.
6. If the **pendingxmlidentifier** value exists, delete the value.
7. Unload the test hive.
8. Load the system hive, name it as "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 details, see the following Knowledge Base article:

- [969028](#) How to generate a kernel or a complete memory dump file in Windows Server 2008 and Windows Server 2008 R2

For more information about page file problems in Windows 10 or Windows Server 2016, see the following Knowledge Base article:

- [4133658](#) Introduction of page file in Long-Term Servicing Channel and Semi-Annual Channel of Windows

For more information about Stop errors, see the following Knowledge Base article:

- [3106831](#) Troubleshooting Stop error problems for IT Pros

If the dump file shows an error that is related to a driver (for example, windows\system32\drivers\stcvsm.sys is missing or corrupted), follow these guidelines:

- Check the functionality that is provided by the driver. If the driver is a third-party boot driver, make sure that you understand what it does.
- If the driver is not 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, open WinRE, open a command prompt, and then run the following command:

```
SFC /Scannow /OffBootDir=C:\ /OffWinDir=E:\Windows
```

For more information, see [Using System File Checker \(SFC\) To Fix Issues](#)

- If there is disk corruption, run the check disk command:

```
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.

Advanced troubleshooting for Windows-based computer freeze issues

6/18/2019 • 11 minutes to read • [Edit Online](#)

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.

Identify the problem

- Which computer is freezing? (Example: The impacted computer is a physical server, virtual server, and so on.)
- What operation was being performed when the freezes occurred? (Example: This issue occurs when you shut down GUI, perform one or more operations, and so on.)
- How often do the errors occur? (Example: This issue occurs every night at 7 PM, every day around 7 AM, and so on.)
- On how many computers does this occur? (Example: All computers, only one computer, 10 computers, and so on.)

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 Remote Desktop, Citrix, and so on.
- Use the domain account or local administrator account to log on the computer by using one of the Remote Physical Console Access features, such as Dell Remote Access Card (DRAC), HP Integrated Lights-Out (iLo), or IBM Remote supervisor adapter (RSA).
- Test ping to the computer. Packet dropping and high network latency may be observed.
- Access administrative shares (**ServerName**\c\$).
- Press Ctrl + Alt + Delete command and check response.
- Try to use Remote Admin tools such as Computer Management, remote Server Manager, and Wmimgmt.msc.

For the computer that is 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 is having the issue. Check the event logs for the relevant Event ID:

- Application event log : Application Error (suggesting 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 the perfmon /report command.

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 the perfmon /report command.
- Check 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
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

NOTE

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 is 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. To do this, follow these steps:
 - a. Go to **Run** and enter `Sysdm.cp1`, and then press enter.

- b. In **System Properties**, on the **Advanced** tab, select **Performance > Settings > Advanced**, and then check or change the virtual memory by clicking **Change**.
- c. Go back to **System Properties > Advanced > Settings** in **Startup and Recovery**.
- d. In the **Write Debugging Information** section, select **Complete Memory Dump**.

NOTE

For Windows versions that are earlier than Windows 8 or Windows Server 2012, the Complete Memory Dump type isn't available in the GUI. You have to change it in Registry Editor. To do this, change the value of the following **CrashDumpEnabled** registry entry to **1** (REG_DWORD):

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\CrashDumpEnabled

- 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 megabytes (MB) over the installed RAM (Initial and Maximum Size).

Additionally, you can use the workaround for [space limitations on the system drive in Windows Server 2008](#).
 - g. Make sure that there's more available space on the system drive than there is physical RAM.
2. Enable the CrashOnCtrlScroll registry value to allow the system to generate a dump file by using the keyboard. To do this, follow these steps:

- a. Go to 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. Exit Registry Editor.

- d. Restart the computer.

3. On some physical computers, you may generate a nonmakeable interruption (NMI) from the Web Interface feature (such as DRAC, iLo, and RSA). However, by default, this setting will stop the system without creating a memory dump.

To allow the operating system to generate a memory dump file at an NMI interruption, set the value of the **NMICrashDump** registry entry to **1** (REG_DWORD). Then, restart the computer to apply this change.

NOTE

This is applicable only for Windows 7, Windows Server 2008 R2, and earlier versions of Windows. For Windows 8 Windows Server 2012, and later versions of Windows, the NMICrashDump registry key is no longer required, and an NMI interruption will result in [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 or verify that the file was created correctly. You can use the Microsoft DumpChk (Crash Dump File Checker) tool to verify that the memory dump files are not corrupted or invalid.

- [Using DumpChk](#)
- [Download DumpCheck](#)

Learn how to use Dumpchk.exe to check your dump files:

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:

```
Logman create counter LOGNAME_Long -u DOMAIN\USERNAME * -f bincirc -v mmdhmm -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
```

```
Logman create counter LOGNAME_Short -u DOMAIN\USERNAME * -f bincirc -v mmdhmm -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:

```
logman start LOGNAME_Long / LOGNAME_Short  
logman stop LOGNAME_Long / LOGNAME_Short
```

The Performance Monitor log is located in the path: C:\PERFLOGS

Method 4: Microsoft Support Diagnostics

1. In the search box of the [Microsoft Support Diagnostics Self-Help Portal](#), type Windows Performance Diagnostic.
2. In the search results, select **Windows Performance Diagnostic**, and then click **Create**.
3. Follow the steps of the diagnostic.

Additional 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. To do this, follow these steps:

NOTE

If it isn't possible to access the affected computer through the network, try to generate a memory dump file through NMI interruption. 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 operating system isn't possible, try to access Registry Editor on the computer remotely in order to check the type of memory dump file and page file with which the computer is currently configured.

- b. From a remote computer that is preferably in the same network and subnet, go to **Registry Editor > Connect Network Registry**. Then, connect to the concerned 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 capabilities (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 (Example value: ?:\pagefile.sys).

If the page file is customized, the size will be reflected in the registry, such as '?:\pagefile.sys 1024 1124' where 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 (such as **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 is physical RAM.
2. Enable the **CrashOnCtrlScroll** registry value on the computer to allow the system to generate a dump file by using the keyboard. To do this, follow these steps:
 - a. From a remote computer preferably in the same network and subnet, go to Registry Editor > Connect Network Registry. Connect to the concerned 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. Exit Registry Editor.
 - d. 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`.

Learn [how to use Pool Monitor](#) and how to [use the data to troubleshoot pool leaks](#).

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

If the virtual machine is running Windows 8, Windows Server 2012, or a later version of Windows on Microsoft Hyper-V Server 2012, you can 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:

```
Debug-VM -Name "VM Name" -InjectNonMaskableInterrupt -ComputerName Hostname
```

NOTE

This method is applicable only to Windows 8, Windows Server 2012, and later versions of Windows virtual machines. For the earlier versions of Windows, see methods 1 through 4 that are described earlier in this section.

You can use VMware Snapshots or suspend state and extract a memory dump file equivalent to a complete memory dump file. By using [Checkpoint To Core Tool \(vmss2core\)](#), you can convert both suspend (.vmss) and snapshot (.vmsn) state files to a dump file and 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 that's described in Method 1 and on [the Citrix site](#).

Space limitations on the system drive in Windows Server 2008

On Windows Server 2008, you may not have enough free disk space to generate a complete memory dump file on the system volume. There's a [hotfix](#) that allows for the data collection even though there isn't sufficient space on the system drive to store the memory dump file.

Additionally, on Windows Server 2008 Service Pack (SP2), there's a second option if the system drive doesn't have sufficient space. Namely, you can use the DedicatedDumpFile registry entry. To learn how to use the registry entry, see [New behavior in Windows Vista and Windows Server 2008](#).

For more information, see [How to use the DedicatedDumpFile registry value to overcome space limitations on the system drive](#).

Advanced troubleshooting for Stop error or blue screen error issue

6/18/2019 • 19 minutes to read • [Edit Online](#)

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](#).

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 is 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 are not caused by Microsoft Windows components. Instead, these errors are generally related to malfunctioning hardware drivers or drivers that are installed by third-party software. This includes video cards, wireless network cards, security programs, and so on.

Our analysis of the root causes of crashes indicates the following:

- 70 percent are caused by third-party driver code
- 10 percent are caused by hardware issues
- 5 percent are caused by Microsoft code
- 15 percent have unknown causes (because the memory is too corrupted to analyze)

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. As a best practice, we recommend that you do the following:
 - a. 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:
 - [Windows 10, version 1809](#)
 - [Windows 10, version 1803](#)
 - [Windows 10, version 1709](#)
 - [Windows 10, version 1703](#)
 - [Windows Server 2016 and Windows 10, version 1607](#)

- [Windows 10, version 1511](#)
 - [Windows Server 2012 R2 and Windows 8.1](#)
 - [Windows Server 2008 R2 and Windows 7 SP1](#)
- b. Make sure that the BIOS and firmware are up-to-date.
 - c. Run any relevant hardware and memory tests.
3. Run the [Machine Memory Dump Collector](#) Windows diagnostic package. This diagnostic tool is used to collect machine memory dump files and check for known solutions.
 4. Run [Microsoft Safety Scanner](#) or any other virus detection program that includes checks of the Master Boot Record for infections.
 5. Make sure that there is sufficient free space on the hard disk. The exact requirement varies, but we recommend 10 to 15 percent free disk space.
 6. 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 are 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, it is recommended that you disable the related service.

To do this, 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. [Download DumpConfigurator tool](#).
2. Extract the .zip file and navigate to **Source Code** folder.
3. Run the tool DumpConfigurator.hta, and then select **Elevate this HTA**.
4. Select **Auto Config Kernel**.
5. Restart the computer for the setting to take effect.
6. Stop and disable Automatic System Restart Services (ASR) to prevent dump files from being written.
7. If the server is virtualized, disable auto reboot after the memory dump file is created. This 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 greyed out)
Small memory dump file (256kb)	%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 DumpChk (Crash Dump File Checker) tool to verify that the memory dump files are not corrupted or invalid. For more information, see the following video:

More information on how to use Dumpchk.exe to check your dump files:

- [Using DumpChk](#)
- [Download DumpCheck](#)

Pagefile Settings

- [Introduction of page file in Long-Term Servicing Channel and Semi-Annual Channel of Windows](#)
- [How to determine the appropriate page file size for 64-bit versions of Windows](#)
- [How to generate a kernel or a complete memory dump file in Windows Server 2008 and Windows Server 2008 R2](#)

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 a variety of 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 are not 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, see [Advanced Windows Debugging](#) and [Debugging Kernel Mode Crashes and Hangs](#). Also see the advanced references listed below.

Advanced debugging references

[Advanced Windows Debugging](#)
[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. See the steps [here](#) for more information.
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**. This will install the WinDbg tool.
5. Open the WinDbg tool and set the symbol path by clicking **File** and then clicking **Symbol File Path**.
 - a. If the computer is connected to the Internet, enter the [Microsoft public symbol server](https://msdl.microsoft.com/download/symbols) (<https://msdl.microsoft.com/download/symbols>) and click **OK**. This is the recommended method.
 - b. If the computer is not connected to the Internet, you must specify a local [symbol path](#).
6. Click on **Open Crash Dump**, and then open the memory.dmp file that you copied. See the example below.

```

Microsoft (R) Windows Debugger Version 10.0.17134.12 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.

Loading Dump File [E:\dmp\MEMORY.DMP]
Kernel Bitmap Dump File: Kernel address space is available, User address space may not be available.

Symbol search path is: srv*
Executable search path is:
Windows 10 Kernel Version 16299 MP (8 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 16299.15.amd64fre.rs3_release.170928-1534
Machine Name:
Kernel base = 0xfffff800`9dd07000 PsLoadedModuleList = 0xfffff800`9e06e110
Debug session time: Thu May 10 13:21:48.397 2018 (UTC - 7:00)
System Uptime: 0 days 0:49:58.467
Loading Kernel Symbols
.....
.....
.....
Loading User Symbols
.....

Loading unloaded module list
.....
*****
*
*           Bugcheck Analysis           *
*
*****

Use !analyze -v to get detailed debugging information.

BugCheck EF, {ffffa586380c1580, 0, 0, 0}

Probably caused by : ntdll.dll ( ntdll!RtlpHpFreeWithExceptionProtection$filt$0+44 )

Followup:      MachineOwner
-----

5: kd>

```

7. There should be a link that says **!analyze -v** under **Bugcheck Analysis**. Click that link. This will enter the command `!analyze -v` in the prompt at the bottom of the page.
8. A detailed bugcheck analysis will appear. See the example below.

```
Command - Dump E:\dmp\MEMORY.DMP - WinDbg:10.0.17134.12 AMD64
Followup:      MachineOwner
-----
5: kd> !analyze -v
*****
*                                     *
*                               Bugcheck Analysis                               *
*                                     *
*****

CRITICAL_PROCESS_DIED (ef)
  A critical system process died
Arguments:
Arg1: fffffa586380c1580, Process object or thread object
Arg2: 0000000000000000, If this is 0, a process died. If this is 1, a thread died.
Arg3: 0000000000000000
Arg4: 0000000000000000

Debugging Details:
-----

KEY_VALUES_STRING: 1

TIMELINE_ANALYSIS: 1

DUMP_CLASS: 1
DUMP_QUALIFIER: 401
BUILD_VERSION_STRING: 16299.15.amd64fre.rs3_release.170928-1534
SYSTEM_MANUFACTURER: Dell Inc.
SYSTEM_PRODUCT_NAME: XPS 8700
SYSTEM_SKU: 0x05B7
BIOS_VENDOR: Dell Inc.
BIOS_VERSION: A12
BIOS_DATE: 02/05/2018
BASEBOARD_MANUFACTURER: Dell Inc.
BASEBOARD_PRODUCT: 0KWV78
BASEBOARD_VERSION: A02
DUMP_TYPE: 1
BUGCHECK_P1: fffffa586380c1580
BUGCHECK_P2: 0

5: kd>
```

9. Scroll down to the section where it says **STACK_TEXT**. 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 and if applicable what service is crashing the DLL.

10. See [Using the !analyze Extension](#) for details about how to interpret the STACK_TEXT output.

There are many possible causes of a bugcheck 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:

(HEX data is removed here and lines are numbered for clarity)


```
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
```

The problem here is with **mpssvc** which is a component of the Windows Firewall. The problem was repaired by disabling the firewall temporarily and then resetting firewall policies.

Additional examples are provided in the [Debugging examples](#) section at the bottom of this article.

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 to let that part of the code be examined further.

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 can degrade performance and make the system unusable. This also limits the effectiveness of the tool.

Use the following guidelines when you use Driver Verifier:

- Test any "suspicious" drivers (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 to 20 drivers.
- Additionally, if the computer cannot boot into the desktop because of Driver Verifier, you can disable the tool by starting in Safe mode. This is because the tool cannot 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 table lists general troubleshooting procedures for common Stop error codes.

STOP ERROR MESSAGE AND CODE	MITIGATION
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 0x000000D1	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 NIC driver. Virtualized VMware systems often run "Intel(R) PRO/1000 MT Network Connection" (e1g6032e.sys). This driver is available at http://downloadcenter.intel.com . Contact the hardware vendor to update the NIC driver for a resolution. For VMware systems, use the VMware integrated NIC driver (types VMXNET or VMXNET2 , VMXNET3 can be used) instead of Intel e1g6032e.sys.
PAGE_FAULT_IN_NONPAGED_AREA Stop error code 0x00000050	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. You must 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.

STOP ERROR MESSAGE AND CODE	MITIGATION
<p>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.</p>	<p>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.</p>
<p>NTFS_FILE_SYSTEM Stop error code 0x00000024</p>	<p>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, right-click the drive that you want to scan, select Properties, select Tools, and then select the Check now button. We also suggest that you update the NTFS file system driver (Ntfs.sys), and apply the latest cumulative updates for the current operating system that is experiencing the problem.</p>
<p>KMODE_EXCEPTION_NOT_HANDLED Stop error code 0x0000001E</p>	<p>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.</p> <p>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 do this, follow these steps:</p> <p>Go to Settings > Update & security > Recovery. Under Advanced startup, select Restart now. After your PC restarts to the Choose an option screen, select Troubleshoot > Advanced options > Startup Settings > Restart. After the computer restarts, you'll see a list of options. Press 4 or F4 to start the computer in Safe mode. Or, if you intend to use the Internet while in Safe mode, press 5 or F5 for the Safe Mode with Networking option.</p>
<p>DPC_WATCHDOG_VIOLATION Stop error code 0x00000133</p>	<p>This Stop error code is caused by a faulty driver that does not complete its work within the allotted time frame in certain conditions. To enable us 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 additional error messages that might help identify the device or driver that is causing Stop error 0x133. Verify that any new hardware that is 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, and 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.</p>

STOP ERROR MESSAGE AND CODE	MITIGATION
<p>USER_MODE_HEALTH_MONITOR Stop error code 0x0000009E</p>	<p>This Stop error indicates that a user-mode health check failed in a way that prevents graceful shutdown. Therefore, 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.</p> <p>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 is 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 is not 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 will be taken. Review the Cluster logs to identify the process and investigate which items might cause the process to hang. For more information, see "Why is my Failover Clustering node blue screening with a Stop 0x0000009E?" Also, see the following Microsoft video What to do if a 9E occurs.</p>

Debugging examples

Example 1

This bugcheck is caused by a driver hang during upgrade, resulting in a bugcheck D1 in NDIS.sys (a Microsoft driver). The **IMAGE_NAME** will tell you the faulting driver, but since this is Microsoft driver it cannot be replaced or removed. The resolution method is to disable the network device in device manager and try the upgrade again.

```

2: kd> !analyze -v
*****
*
*                               *
*                               *
*                               *
*                               *
*                               *
*****

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: 00000000011092a, memory referenced
Arg2: 000000000000002, IRQL
Arg3: 000000000000001, 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_TELSVCS_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
00000000011092a
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: fffff884c0c3f6b0 -- (.trap 0xfffffa884c0c3f6b0)
NOTE: The trap frame does not contain all registers.
Some register values may be zeroed or incorrect.
rax=fffff807ad018bf0 rbx=0000000000000000 rcx=00000000011090a
rdx=fffff807ad018c10 rsi=0000000000000000 rdi=0000000000000000
rip=fffff807aa74f4c4 rsp=fffffa884c0c3f840 rbp=000000002408fd00
r8=ffffb30e0e99ea30 r9=0000000001d371c1 r10=0000000020000080
r11=0000000000000000 r12=0000000000000000 r13=0000000000000000
r14=0000000000000000 r15=0000000000000000
iop1=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:
fffffa884`c0c3f568 fffff800`603799e9 : 00000000`0000000a 00000000`0011092a 00000000`00000002 00000000`00000001
: nt!KeBugCheckEx [minkernel\ntos\ke\amd64\procstat.asm @ 134]
fffffa884`c0c3f570 fffff800`60377d7d : fffff78a`4000a150 fffffb30e`03fba001 ffff8180`f0b5d180 00000000`000000ff
: nt!KiBugCheckDispatch+0x69 [minkernel\ntos\ke\amd64\trap.asm @ 2998]
fffffa884`c0c3f6b0 fffff807`aa74f4c4 : 00000000`00000002 ffff8180`f0754180 00000000`00269fb1 ffff8180`f0754180
: nt!KiPageFault+0x23d [minkernel\ntos\ke\amd64\trap.asm @ 1248]
fffffa884`c0c3f840 fffff800`60256b63 : fffffb30e`0e18f710 ffff8180`f0754180 fffffa884`c0c3fa18 00000000`00000002
: NDIS!NdisQueueIoWorkItem+0x4 [minio\ndis\sys\miniport.c @ 9708]
fffffa884`c0c3f870 fffff800`60257bfd : 00000000`00000008 00000000`00000000 00000000`00269fb1 ffff8180`f0754180
: nt!KiProcessExpiredTimerList+0x153 [minkernel\ntos\ke\dpcsup.c @ 2078]
fffffa884`c0c3f960 fffff800`6037123a : 00000000`00000000 ffff8180`f0754180 00000000`00000000 ffff8180`f0760cc0
: nt!KiRetireDpcList+0x43d [minkernel\ntos\ke\dpcsup.c @ 1512]
fffffa884`c0c3fb60 00000000`00000000 : fffffa884`c0c40000 fffffa884`c0c39000 00000000`00000000 00000000`00000000
: nt!KiIdleLoop+0x5a [minkernel\ntos\ke\amd64\idle.asm @ 166]

RETRACER ANALYSTS TAG STATUS: Failed in getting KPCR for core 2
```

```

NETWORK_ANALYSIS_TAG_STATUS: Failed in getting PCR for CORE 2
THREAD_SHA1_HASH_MOD_FUNC: 5b59a784f22d4b5cbd5a8452fe39914b8fd7961d
THREAD_SHA1_HASH_MOD_FUNC_OFFSET: 5643383f9cae3ca39073f7721b53f0c633bf948
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
BUILDDATESTR: 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!ndisqueuioworkitem
FAILURE_ID_HASH: {10686423-afa1-4852-ad1b-9324ac44ac96}
FAILURE_ID_REPORT_LINK: http://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.

```
1: kd> !analyze -v
```

```
*****  
*                                                                 *  
*                               Bugcheck Analysis                    *  
*                                                                 *  
*****
```

PAGE_FAULT_IN_NONPAGED_AREA (50)

Invalid system memory was referenced. This cannot 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\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\crt\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!ndisPnPStartDevice+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!IoCallDriver+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+0xcfc [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: 44dc639eb162a28d47eaeae4afe6f9eccc3d
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_WDDM1.3_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
BUILDDATESTR: 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: http://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](#)

Advanced troubleshooting for Stop error 7B or Inaccessible_Boot_Device

6/26/2019 • 8 minutes to read • [Edit Online](#)

This article provides steps to troubleshoot **Stop error 7B: Inaccessible_Boot_Device**. This error may occur after some changes are made to the computer, or immediately after you deploy Windows on the computer.

Causes of the Inaccessible_Boot_Device Stop error

Any one of the following factors may 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 because of Component Based Store corruptions
- Corrupted files in the **Boot** partition (for example, corruption in the volume that is labeled **SYSTEM** when you run the `diskpart` > `list vol` command)

Troubleshoot this error

Start the computer in [Windows Recovery Mode \(WinRE\)](#). To do this, follow 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:

```
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 will not 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:

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 is not listed in the output, you will 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, 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.

An example output if the computer is UEFI-based:

device	partition=\Device\HarddiskVolume2
path	\EFI\Microsoft\Boot\bootmgfw.efi

An example output if the machine is BIOS based:

Device	partition=C:
--------	--------------

NOTE

This output may 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 **bootmgr** and **winload** entries under **{default}** will contain an **.efi** extension.

```
X:\Sources>bcdedit

Windows Boot Manager
-----
identifier                {bootmgr}
device                    partition=\Device\HarddiskVolume2
path                      \EFI\Microsoft\Boot\bootmgfw.efi
description               Windows Boot Manager
locale                    en-US
inherit                   {globalsettings}
integrityservices        Enable
default                   {default}
resumeobject              {794a37b9-6ff0-11e6-8ad9-8d64679fc580}
displayorder              {default}
toolsdisplayorder         {memdiag}
timeout                   30

Windows Boot Loader
-----
identifier                {default}
device                    partition=C:
path                      \Windows\system32\winload.efi
description               Windows 8.1
locale                    en-US
inherit                   {bootloadersettings}
recoverysequence         {794a37bd-6ff0-11e6-8ad9-8d64679fc580}
integrityservices        Enable
recoveryenabled           Yes
isolatedcontext           Yes
allowedinmemorysettings  0x15000075
osdevice                  partition=C:
systemroot                \Windows
resumeobject              {794a37b9-6ff0-11e6-8ad9-8d64679fc580}
nx                        OptOut
pae                       ForceDisable
bootmenupolicy            Standard
```

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 is 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 is completed, run the following command to make the changes:

```
bcdedit /set *{identifier}* option value
```

For example, if the device under {default} is wrong or missing, run the following command to set it:

```
bcdedit /set {default} device partition=C:
```

If you want to re-create the BCD completely, 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 per the path that is specified in the **bcdedit** command. By default, **bootmgr** in the BIOS partition will be 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, as follows:

```
D:\> Mkdir BootBackup
R:\> Copy *.* D:\BootBackup
```

2. If you are using Windows 10, or if you are 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, as follows:

```
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, this command would be the following:

```
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 do not have a Windows 10 ISO, you must format the partition and copy **bootmgr** from another working computer that has a similar Windows build. To do this, follow these steps:

1. Start **Notepad** .
2. Press Ctrl+O.
3. Navigate to the system partition (in this example, it is 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:

```
Dism /Image:<Specify the OS drive>: /Get-packages
```

After you run this command, you will see the **Install pending** and ****Uninstall Pending**** packages:

```

Package Identity : Package_for_KB4459941~31bf3856ad364e35~amd64~~6.3.1.2285
State : Install Pending
Release Type : Update
Install Time : 11/13/2018 7:41 PM

Package Identity : Package_for_KB4462930~31bf3856ad364e35~amd64~~6.3.1.0
State : Installed
Release Type : Update
Install Time : 11/7/2018 4:54 PM

Package Identity : Package_for_KB4467694~31bf3856ad364e35~amd64~~6.3.1.0
State : Installed
Release Type : Security Update
Install Time : 11/13/2018 7:40 PM

Package Identity : Package_for_RollupFix~31bf3856ad364e35~amd64~~9600.18874.1.4
State : Superseded
Release Type : Security Update
Install Time : 11/7/2018 3:12 PM

Package Identity : Package_for_RollupFix~31bf3856ad364e35~amd64~~9600.19155.1.5
State : Uninstall Pending
Release Type : Security Update
Install Time : 11/7/2018 4:54 PM

Package Identity : Package_for_RollupFix~31bf3856ad364e35~amd64~~9600.19182.1.6
State : Install Pending
Release Type : Security Update
Install Time : 11/13/2018 7:43 PM

```

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

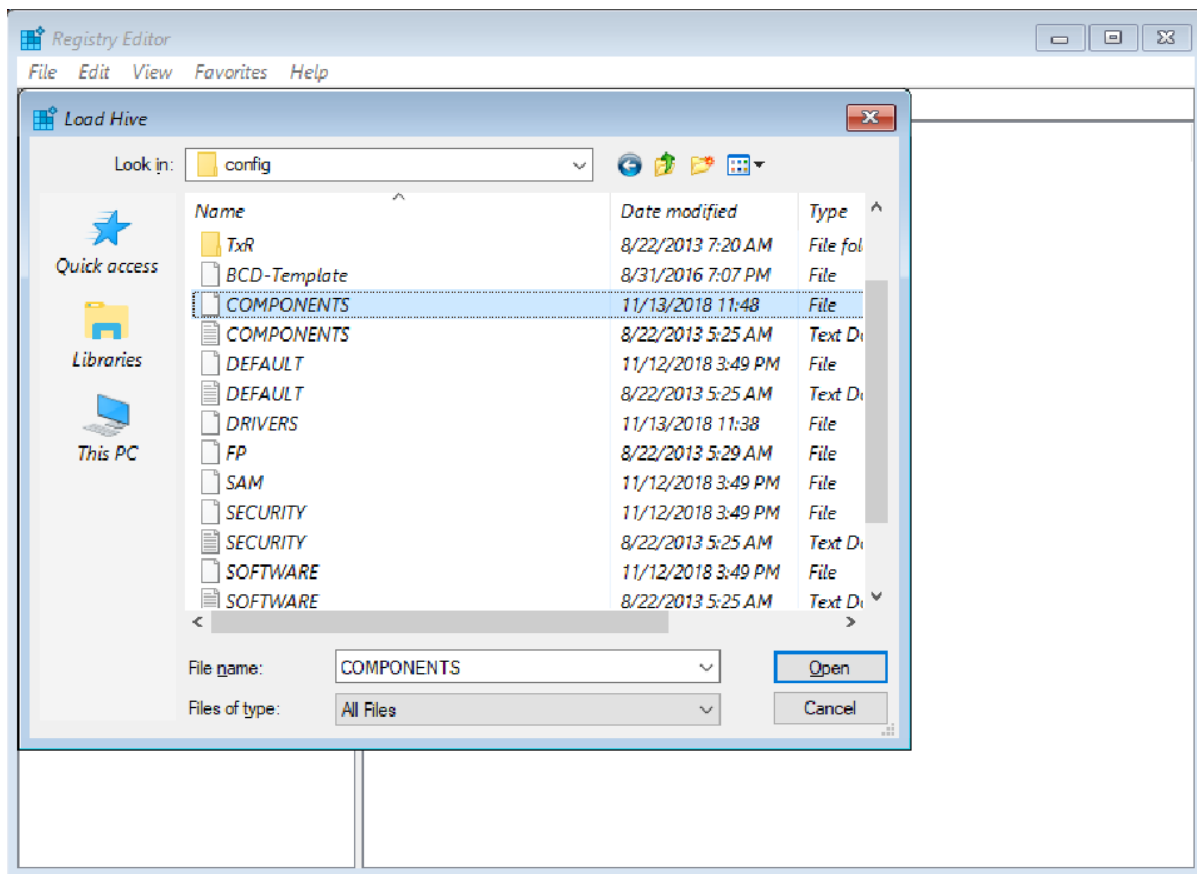
Image Version: 6.3.9600.17709

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.

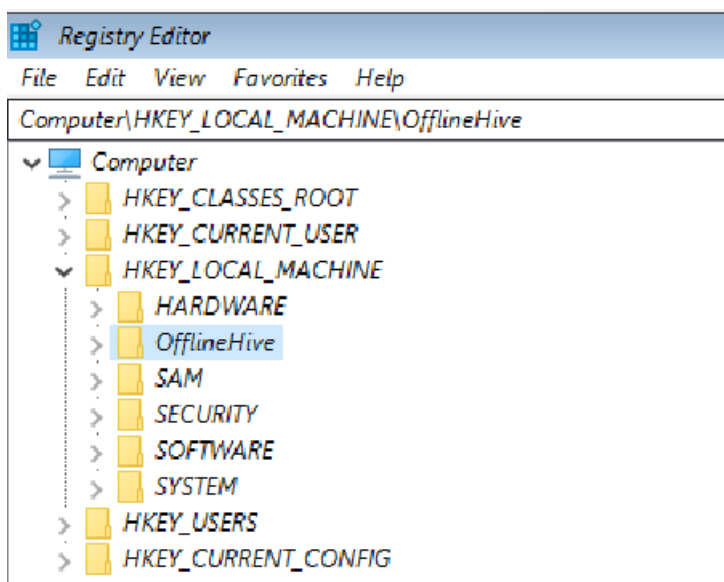
Reverting pending actions from the image...
The operation completed. Revert of pending actions will be attempted after the reboot.
The operation completed successfully.

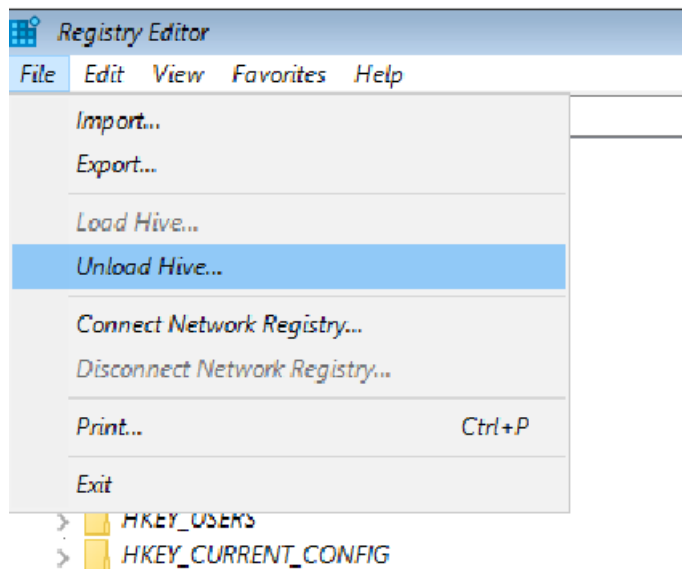
```

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 is named **COMPONENT** (with no extension), and then select **Open**. When you are prompted, enter the name **OfflineComponentHive** for the new hive



- 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.
- Unload the hive. To do this, 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 is named **SYSTEM** (with no extension), and then select **Open** . When you are 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 is **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 an Windows Update installation" section. (Step 11 does not apply to this procedure.)
2. Expand **Services**.
3. Make sure that the following registry keys exist under **Services**:
 - ACPI
 - DISK
 - VOLMGR
 - PARTMGR
 - VOLSNAPE
 - VOLUME

If these keys exist, check each one to make sure that it has a value that is named **Start** and that it is set to **0**. If not, set the value to **0**.

If any of these keys do not exist, you can try to replace the current registry hive by using the hive from **RegBack**. To do this, run the following commands:


```
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 do not 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**.

The following are some of the different registry entries in which you may find these filter drivers. These entries are located 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}

Name	Type	Data
(Default)	REG_SZ	(value not set)
Class	REG_SZ	DiskDrive
ClassDesc	REG_SZ	@%SystemRoot%\System32\StorProp.dll,-17000
EnumPropPages	REG_SZ	StorProp.Dll,DiskPropPageProvider
IconPath	REG_MULTI_SZ	%SystemRoot%\System32\imageres.dll,-32
LastDeleteDate	REG_BINARY	71 7e 26 2f 8e 03 d2 01
LowerFilters	REG_MULTI_SZ	EhStorClass
NoInstallClass	REG_SZ	1
SilentInstall	REG_SZ	1
UpperFilters	REG_MULTI_SZ	PartMgr

If an **UpperFilters** or **LowerFilters** entry is non-standard (for example, it is not a Windows default filter driver, such as PartMgr), remove the entry by double-clicking it in the right pane, and then deleting only that value.

NOTE

There could be multiple entries.

The reason that these entries may affect us is because there may be an entry in the **Services** branch that has a START type set to 0 or 1 (indicating that it is loaded at the Boot or Automatic part of the boot process). Also, either the file that is referred to is missing or corrupted, or it may be named differently than what is listed in the entry.

NOTE

If there actually is a service that is 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 does not start, you can try to run a **chkdisk** process on the system drive, and also run System File Checker. To do this, run the following commands at a WinRE command prompt:

- `chkdisk /f /r 0sDrive:`

```
X:\Sources>chkdisk /f /r C:
The type of the file system is NTFS.

Stage 1: Examining basic file system structure ...
Progress: 20780 of 255744 done; Stage: 8%; Total: 0%; ETA: 5:07:15 ...
```

- `sfc /scannow /offbootdir=0sDrive:\ /offwindir=0sDrive:\Windows`

```
X:\Sources>sfc /scannow /offbootdir=F:\ /offwindir=C:\Windows
Beginning system scan. This process will take some time.
```

Mobile device management

6/18/2019 • 2 minutes to read • [Edit Online](#)

Windows 10 provides an enterprise management solution to help IT pros manage company security policies and business applications, while avoiding compromise of the users' privacy on their personal devices. A built-in management component can communicate with the management server.

There are two parts to the Windows 10 management component:

- The enrollment client, which enrolls and configures the device to communicate with the enterprise management server.
- The management client, which periodically synchronizes with the management server to check for updates and apply the latest policies set by IT.

Third-party MDM servers can manage Windows 10 by using the MDM protocol. The built-in management client is able to communicate with a third-party server proxy that supports the protocols outlined in this document to perform enterprise management tasks. The third-party server will have the same consistent first-party user experience for enrollment, which also provides simplicity for Windows 10 users. MDM servers do not need to create or download a client to manage Windows 10. For details about the MDM protocols, see [\[MS-MDM\]: Mobile Device Management Protocol](#) and [\[MS-MDE2\]: Mobile Device Enrollment Protocol Version 2](#).

MDM security baseline

With Windows 10, version 1809, Microsoft is also releasing a Microsoft MDM security baseline that functions like the Microsoft GP-based security baseline. You can easily integrate this baseline into any MDM to support IT pros' operational needs, addressing security concerns for modern cloud-managed devices.

NOTE

Intune support for the MDM security baseline is coming soon.

The MDM security baseline includes policies that cover the following areas:

- Microsoft inbox security technology (not deprecated) such as Bitlocker, SmartScreen, and DeviceGuard (virtual-based security), ExploitGuard, Defender, and Firewall
- Restricting remote access to devices
- Setting credential requirements for passwords and PINs
- Restricting use of legacy technology
- Legacy technology policies that offer alternative solutions with modern technology
- And much more

For more details about the MDM policies defined in the MDM security baseline and what Microsoft's recommended baseline policy values are, see:

- [MDM Security baseline for Windows 10, version 1903](#)
- [MDM Security baseline for Windows 10, version 1809](#)

For information about the MDM policies defined in the Intune security baseline public preview, see [Windows security baseline settings for Intune](#)

Learn about migrating to MDM

When an organization wants to move to MDM to manage devices, they should prepare by analyzing their current Group Policy settings to see what they need to transition to MDM management. Microsoft created the [MDM Migration Analysis Tool](#) (MMAT) to help. MMAT determines which Group Policies have been set for a target user or computer and then generates a report that lists the level of support for each policy settings in MDM equivalents. For more information, see [MMAT Instructions](#).

Learn about device enrollment

- [Mobile device enrollment](#)
- [Federated authentication device enrollment](#)
- [Certificate authentication device enrollment](#)
- [On-premise authentication device enrollment](#)

Learn about device management

- [Azure Active Directory integration with MDM](#)
- [Enterprise app management](#)
- [Mobile device management \(MDM\) for device updates](#)
- [Enable offline upgrades to Windows 10 for Windows Embedded 8.1 Handheld devices](#)
- [OMA DM protocol support](#)
- [Structure of OMA DM provisioning files](#)
- [Server requirements for OMA DM](#)
- [Enterprise settings, policies, and app management](#)

Learn about configuration service providers

- [Configuration service provider reference](#)
- [WMI providers supported in Windows 10](#)
- [Using PowerShell scripting with the WMI Bridge Provider](#)
- [MDM Bridge WMI Provider](#)

Change history for Client management

5/31/2019 • 2 minutes to read • [Edit Online](#)

This topic lists new and updated topics in the [Client management](#) documentation for Windows 10 and Windows 10 Mobile.

December 2018

NEW OR CHANGED TOPIC	DESCRIPTION
Advanced troubleshooting for TCP/IP	New
Collect data using Network Monitor	New
Troubleshoot TCP/IP connectivity	New
Troubleshoot port exhaustion issues	New
Troubleshoot Remote Procedure Call (RPC) errors	New

November 2018

NEW OR CHANGED TOPIC	DESCRIPTION
Advanced troubleshooting for Windows-based computer freeze issues	New
Advanced troubleshooting for Stop error or blue screen error issue	New

RELEASE: Windows 10, version 1709

The topics in this library have been updated for Windows 10, version 1709 (also known as the Fall Creators Update).

July 2017

NEW OR CHANGED TOPIC	DESCRIPTION
Group Policy settings that apply only to Windows 10 Enterprise and Education Editions	Added that Start layout policy setting can be applied to Windows 10 Pro, version 1703

June 2017

NEW OR CHANGED TOPIC	DESCRIPTION
Create mandatory user profiles	Added Windows 10, version 1703, to profile extension table

April 2017

NEW OR CHANGED TOPIC	DESCRIPTION
New policies for Windows 10	Added a list of new Group Policy settings for Windows 10, version 1703

RELEASE: Windows 10, version 1703

The topics in this library have been updated for Windows 10, version 1703 (also known as the Creators Update).

The following new topic has been added:

- [Manage the Settings app with Group Policy](#)