Manage connections from Windows 10 and Windows 11 operating system components to Microsoft services

- Article
- 06/18/2022
- 61 minutes to read
-

Applies to

- Windows 11 Enterprise
- Windows 10 Enterprise, version 1607 and later
- Windows Server 2016
- Windows Server 2019

This article describes the network connections that Windows 10 and Windows 11 components make to Microsoft and the Windows Settings, Group Policies and registry settings available to IT Professionals to help manage the data shared with Microsoft. If you want to minimize connections from Windows to Microsoft services, or configure privacy settings, there are a number of settings for consideration. For example, you can configure diagnostic data to the lowest level for your edition of Windows and evaluate other connections Windows makes to Microsoft services you want to turn off using the instructions in this article. While it is possible to minimize network connections to Microsoft, there are many reasons why these communications are enabled by default, such as updating malware definitions and maintaining current certificate revocation lists. This data helps us deliver a secure, reliable, and up-to-date experience.

Microsoft provides a Windows Restricted Traffic Limited Functionality Baseline package that will allow your organization to quickly configure the settings covered in this document to restrict connections from Windows 10 and Windows 11 to Microsoft. The Windows Restricted Traffic Limited Baseline is based on Group Policy Administrative Template functionality and the package you download contains further instructions on how to deploy to devices in your organization. Since some of the settings can reduce the functionality and security configuration of your device, **before deploying Windows Restricted Traffic Limited Functionality Baseline** make sure you **choose the right settings configuration for your environment** and **ensure that Windows and Microsoft Defender Antivirus are fully up to date**. Failure to do so may result in errors or unexpected behavior. You should not extract this package to the windows\system32 folder because it will not apply correctly.

Important

- The downloadable Windows 10, version 1903 scripts/settings can be used on Windows 10, version 1909 devices.
- The Allowed Traffic endpoints are listed here: Allowed Traffic
    - CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol) network traffic cannot be disabled and will still show up in network traces. CRL and OCSP checks are made to the issuing certificate authorities. Microsoft is one

of these authorities. There are many others such as DigiCert, Thawte, Google, Symantec, and VeriSign.

- For security reasons, it is important to take care in deciding which settings to configure as some of them may result in a less secure device. Examples of settings that can lead to a less secure device configuration include: Windows Update, Automatic Root Certificates Update, and Microsoft Defender Antivirus. Accordingly, we do not recommend disabling any of these features.
- It is recommended that you restart a device after making configuration changes to it.
- The **Get Help** and **Give us Feedback** links no longer work after the Windows Restricted Traffic Limited Functionality Baseline is applied.

Warning

- If a user executes the **Reset this PC** command (Settings -> Update & Security -> Recovery) with the **Keep my files option** (or the **Remove Everything** option) the Windows Restricted Traffic Limited Functionality Baseline settings will need to be re-applied in order to re-restrict the device. Egress traffic may occur prior to the re-application of the Restricted Traffic Limited Functionality Baseline settings.
- To restrict a device effectively (first time or subsequently), it is recommended to apply the Restricted Traffic Limited Functionality Baseline settings package in offline mode.
- During update or upgrade of Windows, egress traffic may occur.

To use Microsoft Intune cloud-based device management for restricting traffic please refer to the Manage connections from Windows 10 and Windows 11 operating system components to Microsoft services using Microsoft Intune MDM Server.

We are always striving to improve our documentation and welcome your feedback. You can provide feedback by contacting **telmhelp@microsoft.com**.

Management options for each setting

The following sections list the components that make network connections to Microsoft services by default. You can configure these settings to control the data that is sent to Microsoft. To prevent Windows from sending any data to Microsoft, configure diagnostic data at the Security level, turn off Microsoft Defender Antivirus diagnostic data and MSRT reporting, and turn off all of these connections

Settings for Windows 10 and Windows 11 Enterprise edition

The following table lists management options for each setting, For Windows 10 (beginning with Windows 10 Enterprise version 1607) and Windows 11.

Important

If you need assistance with troubleshooting issues, please refer to:

- Keep your device running smoothly
- CSP - Troubleshooting

Setting	UI	Group Policy	Registry

Setting	UI	Group Policy	Registry
1. Automatic Root Certificates Update		✓	✓
2. Cortana and Search		✓	✓
3. Date & Time	✓	✓	✓
4. Device metadata retrieval		✓	✓
5. Find My Device	✓	✓	✓
6. Font streaming		✓	✓
7. Insider Preview builds	✓	✓	✓
8. Internet Explorer		✓	✓
9. License Manager			✓
10. Live Tiles		✓	✓
11. Mail synchronization	✓		✓
12. Microsoft Account			✓
13. Microsoft Edge		✓	✓
14. Network Connection Status Indicator		✓	✓
15. Offline maps	✓	✓	✓
16. OneDrive		✓	✓
17. Preinstalled apps	✓		
18. Settings > Privacy & security			
18.1 General	✓	✓	✓
18.2 Location	✓	✓	✓
18.3 Camera	✓	✓	✓
18.4 Microphone	✓	✓	✓
18.5 Notifications	✓	✓	✓
18.6 Speech	✓	✓	✓
18.7 Account info	✓	✓	✓
18.8 Contacts	✓	✓	✓
18.9 Calendar	✓	✓	✓
18.10 Call history	✓	✓	✓

Setting	UI	Group Policy	Registry
18.11 Email	✓	✓	✓
18.12 Messaging	✓	✓	✓
18.13 Phone calls	✓	✓	✓
18.14 Radios	✓	✓	✓
18.15 Other devices	✓	✓	✓
18.16 Feedback & diagnostics	✓	✓	✓
18.17 Background apps	✓	✓	✓
18.18 Motion	✓	✓	✓
18.19 Tasks	✓	✓	✓
18.20 App Diagnostics	✓	✓	✓
18.21 Inking & Typing	✓		✓
18.22 Activity History	✓	✓	✓
18.23 Voice Activation	✓	✓	✓
19. Software Protection Platform		✓	✓
20. Storage Health		✓	✓
21. Sync your settings	✓	✓	✓
22. Teredo		✓	✓
23. Wi-Fi Sense	✓	✓	✓
24. Microsoft Defender Antivirus		✓	✓
25. Windows Spotlight	✓	✓	✓
26. Microsoft Store		✓	✓
27. Apps for websites		✓	✓
28. Delivery Optimization	✓	✓	✓
29. Windows Update		✓	✓
30. Cloud Clipboard		✓	
31. Services Configuration		✓	✓
32. Widgets		✓	✓

Settings for Windows Server 2016 with Desktop Experience

See the following table for a summary of the management settings for Windows Server 2016 with Desktop Experience.

Setting	UI	Group Policy	Registry
1. Automatic Root Certificates Update		✓	✓
2. Cortana and Search		✓	✓
3. Date & Time	✓	✓	✓
4. Device metadata retrieval		✓	✓
6. Font streaming		✓	✓
7. Insider Preview builds	✓	✓	✓
8. Internet Explorer		✓	✓
10. Live Tiles		✓	✓
12. Microsoft Account			✓
14. Network Connection Status Indicator		✓	✓
16. OneDrive		✓	✓
18. Settings > Privacy & security			
19. Software Protection Platform		✓	✓
22. Teredo		✓	✓
24. Microsoft Defender Antivirus		✓	✓
26. Microsoft Store		✓	✓
27. Apps for websites		✓	✓
29. Windows Update		✓	✓

Settings for Windows Server 2016 Server Core

See the following table for a summary of the management settings for Windows Server 2016 Server Core.

Setting	Group Policy	Registry
1. Automatic Root Certificates Update	✓	✓
3. Date & Time	✓	✓
6. Font streaming	✓	✓

Setting	Group Policy	Registry
14. Network Connection Status Indicator	✓	✓
19. Software Protection Platform	✓	✓
22. Teredo	✓	✓
24. Microsoft Defender Antivirus	✓	✓
29. Windows Update	✓	✓

Settings for Windows Server 2016 Nano Server

See the following table for a summary of the management settings for Windows Server 2016 Nano Server.

Setting	Registry
1. Automatic Root Certificates Update	✓
3. Date & Time	✓
22. Teredo	✓
29. Windows Update	✓

Settings for Windows Server 2019

See the following table for a summary of the management settings for Windows Server 2019.

Setting	UI	Group Policy	Registry
1. Automatic Root Certificates Update		✓	✓
2. Cortana and Search		✓	✓
3. Date & Time	✓	✓	✓
4. Device metadata retrieval		✓	✓
5. Find My Device	✓	✓	✓
6. Font streaming		✓	✓
7. Insider Preview builds	✓	✓	✓
8. Internet Explorer		✓	✓
10. Live Tiles		✓	✓
11. Mail synchronization	✓		✓
12. Microsoft Account			✓

Setting	UI	Group Policy	Registry
13. Microsoft Edge		✓	✓
14. Network Connection Status Indicator		✓	✓
15. Offline maps	✓	✓	✓
16. OneDrive		✓	✓
17. Preinstalled apps	✓		
18. Settings > Privacy & security			
18.1 General	✓	✓	✓
18.2 Location	✓	✓	✓
18.3 Camera	✓	✓	✓
18.4 Microphone	✓	✓	✓
18.5 Notifications	✓	✓	✓
18.6 Speech	✓	✓	✓
18.7 Account info	✓	✓	✓
18.8 Contacts	✓	✓	✓
18.9 Calendar	✓	✓	✓
18.10 Call history	✓	✓	✓
18.11 Email	✓	✓	✓
18.12 Messaging	✓	✓	✓
18.13 Phone calls	✓	✓	✓
18.14 Radios	✓	✓	✓
18.15 Other devices	✓	✓	✓
18.16 Feedback & diagnostics	✓	✓	✓
18.17 Background apps	✓	✓	✓
18.18 Motion	✓	✓	✓
18.19 Tasks	✓	✓	✓
18.20 App Diagnostics	✓	✓	✓
18.21 Inking & Typing	✓		✓
18.22 Activity History	✓	✓	✓

Setting	UI	Group Policy	Registry
18.23 Voice Activation	✓	✓	✓
19. Software Protection Platform		✓	✓
20. Storage Health		✓	✓
21. Sync your settings	✓	✓	✓
22. Teredo		✓	✓
23. Wi-Fi Sense	✓	✓	✓
24. Microsoft Defender Antivirus		✓	✓
25. Windows Spotlight	✓	✓	✓
26. Microsoft Store		✓	✓
27. Apps for websites		✓	✓
28. Delivery Optimization	✓	✓	✓
29. Windows Update		✓	✓
30. Cloud Clipboard		✓	
31. Services Configuration		✓	✓

How to configure each setting

Use the following sections for more information about how to configure each setting.

1. Automatic Root Certificates Update

The Automatic Root Certificates Update component is designed to automatically check the list of trusted authorities on Windows Update to see if an update is available. For more information, see Automatic Root Certificates Update Configuration. Although not recommended, you can turn off Automatic Root Certificates Update, which also prevents updates to the disallowed certificate list and the pin rules list.

Caution

By not automatically downloading the root certificates the device may not be able to connect to some websites.

For Windows 10, Windows Server 2016 with Desktop Experience, Windows Server 2016 Server Core, and Windows 11:

- Enable the Group Policy: **Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication Settings > Turn off Automatic Root Certificates Update**

-and-

1. Navigate to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Public Key Policies**.
2. Double-click **Certificate Path Validation Settings**.
3. On the **Network Retrieval** tab, select the **Define these policy settings** check box.
4. Clear the **Automatically update certificates in the Microsoft Root Certificate Program (recommended)** check box, and then click **OK**.

-or-

- Create the registry path **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot** and then add a REG_DWORD registry setting, named **DisableRootAutoUpdate**, with a value of 1.

  -and-

1. Navigate to **Computer Configuration** > **Windows Settings** > **Security Settings** > **Public Key Policies**.
2. Double-click **Certificate Path Validation Settings**.
3. On the **Network Retrieval** tab, select the **Define these policy settings** check box.
4. Clear the **Automatically update certificates in the Microsoft Root Certificate Program (recommended)** check box, and then click **OK**.

On Windows Server 2016 Nano Server:

- Create the registry path **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SystemCertificates\AuthRoot** and then add a REG_DWORD registry setting, named **DisableRootAutoUpdate**, with a value of 1.

Note

CRL and OCSP network traffic is currently Allowed Traffic and will still show up in network traces. CRL and OCSP checks are made to the issuing certificate authorities. Microsoft is one of them, but there are many others, such as DigiCert, Thawte, Google, Symantec, and VeriSign.

2. Cortana and Search

Use Group Policies to manage settings for Cortana. For more info, see Cortana, Search, and privacy: FAQ.

2.1 Cortana and Search Group Policies

Find the Cortana Group Policy objects under **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Search**.

Policy	Description
Allow Cortana	Choose whether to let Cortana install and run on the device.

Policy	Description
Allow search and Cortana to use location	**Disable** this policy to turn off Cortana. Choose whether Cortana and Search can provide location-aware search results. **Disable** this policy to block access to location information for Cortana.
Do not allow web search	Choose whether to search the web from Windows Desktop Search. **Enable** this policy to remove the option to search the Internet from Cortana.
Don't search the web or display web results in Search	Choose whether to search the web from Cortana. **Enable** this policy to stop web queries and results from showing in Search.

You can also apply the Group Policies using the following registry keys:

Policy	Registry Path
Allow Cortana	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search REG_DWORD: AllowCortana Value: 0
Allow search and Cortana to use location	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search REG_DWORD: AllowSearchToUseLocation Value: 0
Do not allow web search	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search REG_DWORD: DisableWebSearch Value: 1
Don't search the web or display web results in Search	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search REG_DWORD: ConnectedSearchUseWeb Value: 0

Important

Using the Group Policy editor these steps are required for all supported versions of Windows 10 and Windows 11, however they are not required for devices running Windows 10, version 1607 or Windows Server 2016.

1. Expand **Computer Configuration > Windows Settings > Security Settings > Windows Defender Firewall with Advanced Security > Windows Defender Firewall with Advanced Security - `LDAP name`**, and then click **Outbound Rules**.
2. Right-click **Outbound Rules**, and then click **New Rule**. The **New Outbound Rule Wizard** starts.

3. On the **Rule Type** page, click **Program**, and then click **Next**.
4. On the **Program** page, click **This program path**, type **%windir%\systemapps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe**, and then click **Next**.
    - On Windows 11, type **"%windir%\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe"** instead.
5. On the **Action** page, click **Block the connection**, and then click **Next**.
6. On the **Profile** page, ensure that the **Domain**, **Private**, and **Public** check boxes are selected, and then click **Next**.
7. On the **Name** page, type a name for the rule, such as **Cortana firewall configuration**, and then click **Finish.**
8. Right-click the new rule, click **Properties**, and then click **Protocols and Ports**.
9. Configure the **Protocols and Ports** page with the following info, and then click **OK**.
    - For **Protocol type**, choose **TCP**.
    - For **Local port**, choose **All Ports**.
    - For **Remote port**, choose **All ports**.

-or-

- Create a new REG_SZ registry setting named **{0DE40C8E-C126-4A27-9371-A27DAB1039F7}** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules** and set it to a value of **v2.25|Action=Block|Active=TRUE|Dir=Out|Protocol=6|App=%windir%\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\searchUI.exe|Name=Block outbound Cortana|**
- On Windows 11, follow the previous section instead and use the Group Policy editor.

If your organization tests network traffic, do not use a network proxy as Windows Firewall does not block proxy traffic. Instead, use a network traffic analyzer. Based on your needs, there are many network traffic analyzers available at no cost.

3. Date & Time

You can prevent Windows from setting the time automatically.

- To turn off the feature in the UI: **Settings > Time & language > Date & time > Set time automatically**

  -or-

- Create a REG_SZ registry setting in **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type** with a value of **NoSync**.

After that, configure the following:

- **Disable** the Group Policy: **Computer Configuration > Administrative Templates > System > Windows Time Service > Time Providers > Enable Windows NTP Client**

  -or-

- Create a new REG_DWORD registry setting named **Enabled** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\W32time\TimeProviders\NtpClient** and set it to **0 (zero)**.

4. Device metadata retrieval

To prevent Windows from retrieving device metadata from the Internet:

- **Enable** the Group Policy: **Computer Configuration** > **Administrative Templates** > **System** > **Device Installation** > **Prevent device metadata retrieval from the Internet**.

  -or -

- Create a new REG_DWORD registry setting named **PreventDeviceMetadataFromNetwork** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Device Metadata** and set it to 1 (one).

5. Find My Device

To turn off Find My Device:

- Turn **Off** the feature in the UI by going to **Settings -> Update & Security -> Find My Device**, click the Change button, and set the value to **Off**

  -or-

- **Disable** the Group Policy: **Computer Configuration** > **Administrative Template** > **Windows Components** > **Find My Device** > **Turn On/Off Find My Device**

  -or-

- You can also create a new REG_DWORD registry setting **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FindMyDevice\AllowFindMyDevice** to **0 (zero)**.

6. Font streaming

Fonts that are included in Windows but that are not stored on the local device can be downloaded on demand.

If you're running Windows 10, version 1607, Windows Server 2016, or later:

- **Disable** the Group Policy: **Computer Configuration** > **Administrative Templates** > **Network** > **Fonts** > **Enable Font Providers**.

  -or-

- Create a new REG_DWORD registry setting **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System\EnableFontProviders** to **0 (zero)**.

Note

After you apply this policy, you must restart the device for it to take effect.

7. Insider Preview builds

The Windows Insider Preview program lets you help shape the future of Windows, be part of the community, and get early access to releases of Windows 10 and Windows 11. This setting stops communication with the Windows Insider Preview service that checks for new builds. Windows Insider Preview builds only apply to Windows 10 and Windows 11 and are not available for Windows Server 2016.

Note

If you upgrade a device that is configured to minimize connections from Windows to Microsoft services (that is, a device configured for Restricted Traffic) to a Windows Insider Preview build, the Feedback & Diagnostic setting will automatically be set to **Optional (Full)**. Although the diagnostic data level may initially appear as **Required (Basic)**, a few hours after the UI is refreshed or the machine is rebooted, the setting will become **Optional (Full)**.

To turn off Insider Preview builds for a released version of Windows 10 or Windows 11:

- **Disable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds > Toggle user control over Insider builds**.

To turn off Insider Preview builds for Windows 10 and Windows 11:

Note

If you're running a preview version of Windows 10 or Windows 11, you must roll back to a released version before you can turn off Insider Preview builds.

- Turn off the feature in the UI: **Settings > Update & security > Windows Insider Program > Stop Insider Preview builds**.

  -or-

- **Enable** the Group Policy **Toggle user control over Insider builds** under **Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds**

  -or-

- Create a new REG_DWORD registry setting named **AllowBuildPreview** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PreviewBuilds** with a **value of 0 (zero)**

8. Internet Explorer

Note

When attempting to use Internet Explorer on any edition of Windows Server be aware there are restrictions enforced by Enhanced Security Configuration (ESC). The following Group Policies and Registry Keys are for user interactive scenarios rather than the typical idle traffic scenario. Find the Internet Explorer Group Policy objects under **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer** and make these settings:

Policy	Description
Turn on Suggested Sites	Choose whether an employee can configure Suggested Sites. **Set Value to: Disabled** You can also turn this off in the UI by clearing the **Internet Options** > **Advanced** > **Enable Suggested Sites** check box.
Allow Microsoft services to provide enhanced suggestions as the user types in the Address Bar	Choose whether an employee can configure enhanced suggestions, which are presented to the employee as they type in the Address Bar. **Set Value to: Disabled**
Turn off the auto-complete feature for web addresses	Choose whether auto-complete suggests possible matches when employees are typing web address in the Address Bar. **Set Value to: Enabled** You can also turn this off in the UI by clearing the **Internet Options** > **Advanced** > **Use inline AutoComplete in the Internet Explorer Address Bar and Open Dialog** check box.
Turn off browser geolocation	Choose whether websites can request location data from Internet Explorer. **Set Value to: Enabled**
Prevent managing Microsoft Defender SmartScreen	Choose whether employees can manage the Microsoft Defender SmartScreen in Internet Explorer. **Set Value to: Enabled** and then set **Select Windows Defender SmartScreen mode** to **Off**.

Registry Key	Registry path
Turn on Suggested Sites	HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Suggested Sites REG_DWORD: Enabled **Set Value to: 0**
Allow Microsoft services to provide enhanced suggestions as the user types in the	HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer REG_DWORD: AllowServicePoweredQSA **Set Value to: 0**

Policy	Description
Address Bar	
Turn off the auto-complete feature for web addresses	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete REG_SZ: AutoSuggest Set Value to: **no**
Turn off browser geolocation	HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Geolocation REG_DWORD: PolicyDisableGeolocation **Set Value to: 1**
Prevent managing Microsoft Defender SmartScreen	HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\PhishingFilter REG_DWORD: EnabledV9 **Set Value to: 0**

There are more Group Policy objects that are used by Internet Explorer:

Path	Policy	Description
Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Compatibility View > Turn off Compatibility View	Turn off Compatibility View.	Choose whether an employee can fix website display problems that he or she may encounter while browsing. **Set to: Enabled**
Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Advanced Page	Turn off the flip ahead with page prediction feature	Choose whether an employee can swipe across a screen or click forward to go to the next pre-loaded page of a website. **Set to: Enabled**
Computer Configuration > Administrative Templates > Windows Components > RSS Feeds	Turn off background synchronization for feeds and Web Slices	Choose whether to have background synchronization for feeds and Web Slices. **Set to: Enabled**
Computer Configuration > Administrative Templates > Control Panel > Allow Online Tips	Allow Online Tips	Enables or disables the retrieval of online tips and help for the Settings app. **Set to: Disabled**

You can also use Registry keys to set these policies.

Registry Key	Registry path
Choose whether employees can configure Compatibility View.	HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\BrowserEmulation REG_DWORD: DisableSiteListEditing **Set Value to 1**
Turn off the flip ahead	HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\FlipAhead

Registry Key	Registry path
with page prediction feature	REG_DWORD: Enabled **Set Value to 0**
Turn off background synchronization for feeds and Web Slices	HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Feeds REG_DWORD: BackgroundSyncStatus **Set Value to 0**
Allow Online Tips	HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer REG_DWORD: AllowOnlineTips **Set Value to 0**

To turn off the home page:

- **Enable** the Group Policy: **User Configuration > Administrative Templates > Windows Components > Internet Explorer > Disable changing home page settings**, and set it to **about:blank**

  -or-

- Create a new REG_SZ registry setting named **Start Page** in **HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Internet Explorer\Main** with a **about:blank**

  -and -

- Create a new REG_DWORD registry setting named **HomePage** in **HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Internet Explorer\Control Panel** with a **1 (one)**

To configure the First Run Wizard:

- **Enable** the Group Policy: **User Configuration > Administrative Templates > Windows Components > Internet Explorer > Prevent running First Run wizard**, and set it to **Go directly to home page**

  -or-

- Create a new REG_DWORD registry setting named **DisableFirstRunCustomize** in **HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Internet Explorer\Main** with a **1 (one)**

To configure the behavior for a new tab:

- **Enable** the Group Policy: **User Configuration > Administrative Templates > Windows Components > Internet Explorer > Specify default behavior for a new tab**, and set it to **about:blank**

  -or-

- Create a new REG_DWORD registry setting named **NewTabPageShow** in **HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Internet Explorer\TabbedBrowsing** with a **0 (zero)**

8.1 ActiveX control blocking

ActiveX control blocking periodically downloads a new list of out-of-date ActiveX controls that should be blocked.

You can turn this off by:

- **Enable** the Group Policy: **User Configuration > Administrative Templates > Windows Components > Internet Explorer > Security Features > Add-on Management > Turn off Automatic download of the ActiveX VersionList**

  -or-

- Changing the REG_DWORD registry setting **HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\VersionManager\DownloadVersionList** to **0 (zero)**.

For more info, see Out-of-date ActiveX control blocking.

9. License Manager

You can turn off License Manager related traffic by setting the following registry entry:

- Add a REG_DWORD value named **Start** to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LicenseManager** and set the **value to 4**
- The value 4 is to disable the service. Here are the available options to set the registry:
  - **0x00000000** = Boot
  - **0x00000001** = System
  - **0x00000002** = Automatic
  - **0x00000003** = Manual
  - **0x00000004** = Disabled

10. Live Tiles

To turn off Live Tiles:

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Start Menu and Taskbar > Notifications > Turn Off notifications network usage**

  -or-

- Create a REG_DWORD registry setting named **NoCloudApplicationNotification** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\PushNotifications** with a **value of 1 (one)**

11. Mail synchronization

To turn off mail synchronization for Microsoft Accounts that are configured on a device:

- In **Settings > Accounts > Your email and accounts**, remove any connected Microsoft Accounts.

-or-

- Remove any Microsoft Accounts from the Mail app.

To turn off the Windows Mail app:

- Create a REG_DWORD registry setting named **ManualLaunchAllowed** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Mail** with a **value of 0 (zero)**.

12. Microsoft Account

Use the below setting to prevent communication to the Microsoft Account cloud authentication service. Many apps and system components that depend on Microsoft Account authentication may lose functionality. Some of them could be in unexpected ways. For example, Windows Update will no longer offer feature updates to devices running Windows 10 1709 or higher and Windows 11. See Feature updates are not being offered while other updates are.

To disable the Microsoft Account Sign-In Assistant:

- Change the **Start** REG_DWORD registry setting in **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\wlidsvc** to a value of **4**.

13. Microsoft Edge

Use Group Policies to manage settings for Microsoft Edge. For more info, see Microsoft Edge and privacy: FAQ and Configure Microsoft Edge policy settings on Windows.

For a complete list of the Microsoft Edge policies, see Group Policy and Mobile Device Management (MDM) settings for Microsoft Edge.

13.1 Microsoft Edge Group Policies

Find the Microsoft Edge Group Policy objects under **Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge**.

Policy	Description
Allow Address bar drop-down list suggestions	Choose whether to show the address bar drop-down list **Set to Disabled**
Allow configuration updates for the Books Library	Choose whether configuration updates are done for the Books Library. **Set to Disabled**
Configure Autofill	Choose whether employees can use autofill on websites. **Set to Disabled**
Configure Do Not Track	Choose whether employees can send Do Not Track headers. **Set to Enabled**

Policy	Description
Configure Password Manager	Choose whether employees can save passwords locally on their devices. **Set to Disabled**
Configure search suggestions in Address Bar	Choose whether the Address Bar shows search suggestions. **Set to Disabled**
Configure Windows Defender SmartScreen (Windows 10, version 1703)	Choose whether Microsoft Defender SmartScreen is turned on or off. **Set to Disabled**
Allow web content on New Tab page	Choose whether a new tab page appears. **Set to Disabled**
Configure Start pages	Choose the Start page for domain-joined devices. **Enabled** and **Set this to `<<about:blank>>`**
Prevent the First Run webpage from opening on Microsoft Edge	Choose whether employees see the First Run webpage. **Set to: Enable**
Allow Microsoft Compatibility List	Choose whether to use the Microsoft Compatibility List in Microsoft Edge. **Set to: Disabled**

Alternatively, you can configure the following Registry keys as described:

Registry Key	Registry path
Allow Address Bar drop-down list suggestions	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\ServiceUI REG_DWORD name: ShowOneBox Set to **0**
Allow configuration updates for the Books Library	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\BooksLibrary REG_DWORD name: AllowConfigurationUpdateForBooksLibrary Set to **0**
Configure Autofill	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\Main REG_SZ name: Use FormSuggest Value: **No**
Configure Do Not Track	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\Main REG_DWORD name: DoNotTrack REG_DWORD: **1**
Configure Password Manager	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\Main REG_SZ name: FormSuggest Passwords REG_SZ: **No**
Configure search suggestions in Address	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\SearchScopes REG_DWORD name: ShowSearchSuggestionsGlobal Value: **0**

Registry Key	Registry path
Bar	
Configure Windows Defender SmartScreen (Windows 10, version 1703)	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter REG_DWORD name: EnabledV9 Value: **0**
Allow web content on New Tab page	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\ServiceUI REG_DWORD name: AllowWebContentOnNewTabPage Value: **0**
Configure corporate Home pages	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\Internet Settings REG_SZ name: ProvisionedHomePages Value: **<<about:blank>>**
Prevent the First Run webpage from opening on Microsoft Edge	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\Main REG_DWORD name: PreventFirstRunPage Value: **1**
Choose whether employees can configure Compatibility View.	HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\BrowserEmulation REG_DWORD: MSCompatibilityMode Value: **0**

13.2 Microsoft Edge Enterprise

For a complete list of the Microsoft Edge policies, see Group Policy and Mobile Device Management (MDM) settings for Microsoft Edge.

Important

- The following settings are applicable to Microsoft Edge version 77 or later.
- For details on supported Operating Systems, see Microsoft Edge supported Operating Systems.
- These policies require the Microsoft Edge administrative templates to be applied. For more information on administrative templates for Microsoft Edge, see Configure Microsoft Edge policy settings on Windows.
- Devices must be domain joined for some of the policies to take effect.

Policy	Group Policy Path	Registry Path

Policy	Group Policy Path	Registry Path
SearchSuggestEnabled	Computer Configuration/Administrative Templates/Windows Component/Microsoft Edge - Enable search suggestions **Set to Disabled**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge **REG_DWORD name: SearchSuggestEnabled Set to 0**
AutofillAddressEnabled	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge - Enable AutoFill for addresses **Set to Disabled**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge **REG_DWORD name: AutofillAddressEnabled Set to 0**
AutofillCreditCardEnabled	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge - Enable AutoFill for credit cards **Set to Disabled**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge **REG_DWORD name: AutofillCreditCardEnabled Set to 0**
ConfigureDoNotTrack	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge - Configure Do Not Track **Set to Enabled**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge **REG_DWORD name: ConfigureDoNotTrack Set to 1**
PasswordManagerEnabled	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge/Password manager and protection-Enable saving passwords to the password manager **Set to Disabled**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge **REG_DWORD name: PasswordManagerEnabled Set to 0**
DefaultSearchProviderEnabled	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge/Default search	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge **REG_DWORD name: DefaultSearchProviderEnabled Set to 0**

Policy	Group Policy Path	Registry Path
	provider-Enable the default search provider **Set to Disabled**	
HideFirstRunExperience	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge/Hide the First-run experience and splash screen **Set to Enabled**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge **REG_DWORD name: HideFirstRunExperience Set to 1**
SmartScreenEnabled	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge/SmartScreen settings-Configure Microsoft Defender SmartScreen **Set to Disabled**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge **REG_DWORD name: SmartScreenEnabled Set to 0**
NewTabPageLocation	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge/Startup, home page and new tab page- Configure the new tab page URL **Set to Enabled-Value "about:blank"**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge **REG_SZ name: NewTabPageLocation Set to about:blank**
RestoreOnStartup	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge/Startup, home page and new tab page- Action to take on startup **Set to Disabled**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge **REG_DWORD name: RestoreOnStartup Set to 5**
RestoreOnStartupURLs	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge/Startup, home	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge\RestoreOnStartupURLs **REG_SZ name: 1 Set to about:blank**

Policy	Group Policy Path	Registry Path
	page and new tab page- Sites to open when the browser starts **Set to Disabled**	
UpdateDefault	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge Update/Applications-Update policy override default **Set to Enabled - 'Updates disabled'**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge\EdgeUpdate **REG_DWORD name: UpdateDefault Set to 0**
AutoUpdateCheckPeriodMinutes	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge Update/Preferences-Auto-update check period override **Set to Enabled - Set Value for Minutes between update checks to 0**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge\EdgeUpdate **REG_DWORD name: AutoUpdateCheckPeriodMinutes Set to 0**
Experimentation and Configuration Service	Computer Configurations/Administrative Templates/Windows Component/Microsoft Edge Update/Preferences-Auto-update check period override **Set to RestrictedMode**	HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Microsoft\Edge\EdgeUpdate **REG_DWORD name: ExperimentationAndConfigurationServiceControl Set to 0**

14. Network Connection Status Indicator

Network Connection Status Indicator (NCSI) detects Internet connectivity and corporate network connectivity status. NCSI sends a DNS request and HTTP query to http://www.msftconnecttest.com/connecttest.txt to determine if the device can communicate with the Internet. See the Microsoft Networking Blog to learn more.

In versions of Windows 10 prior to version 1607 and Windows Server 2016, the URL was `http://www.msftncsi.com/ncsi.txt`.

You can turn off NCSI by doing one of the following:

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication Settings > Turn off Windows Network Connectivity Status Indicator active tests**

  Note

  After you apply this policy, you must restart the device for the policy setting to take effect.

-or-

- Create a REG_DWORD registry setting named **NoActiveProbe** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkConnectivityStatusIndicator** with a value of 1 (one).

15. Offline maps

You can turn off the ability to download and update offline maps.

- Turn **Off** the feature in the UI by going to **Settings -> Apps -> Offline maps -> Map updates**, toggle the **Automatically update maps** switch to **Off**

  -or-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Maps > Turn off Automatic Download and Update of Map Data**

  -or-

- Create a REG_DWORD registry setting named **AutoDownloadAndUpdateMapData** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Maps** with a **value of 0 (zero)**.

  -and-

- In Windows 10, version 1607 and later, and Windows 11 **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Maps > Turn off unsolicited network traffic on the Offline Maps settings page**

  -or-

- Create a REG_DWORD registry setting named **AllowUntriggeredNetworkTrafficOnSettingsPage** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Maps** with a value of 0 (zero).

16. OneDrive

To turn off OneDrive in your organization:

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > OneDrive > Prevent the usage of OneDrive for file storage**

  -or-

- Create a REG_DWORD registry setting named **DisableFileSyncNGSC** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\OneDrive** with a value of 1 (one).

  -and-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > OneDrive > Prevent OneDrive from generating network traffic until the user signs in to OneDrive (Enable)**

  -or-

- Create a REG_DWORD registry setting named **PreventNetworkTrafficPreUserSignIn** in **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OneDrive** with a **value of 1 (one)**

17. Preinstalled apps

Some preinstalled apps get content before they are opened to ensure a great experience. You can remove these using the steps in this section.

To remove the News app:

- Right-click the app in Start, and then click **Uninstall**.

  -or-

  Important

  If you have any issues with the following commands, restart the system and try the scripts again.

- Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.BingNews"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}**

  -and-

- Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.BingNews | Remove-AppxPackage**

To remove the Weather app:

- Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online |**

Where-Object {$_.PackageName -Like "Microsoft.BingWeather"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}

-and-

- Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.BingWeather | Remove-AppxPackage**

To remove the Money app:

- Right-click the app in Start, and then click **Uninstall**.

  -or-

- Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.BingFinance"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}**

  -and-

- Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.BingFinance | Remove-AppxPackage**

To remove the Sports app:

- Right-click the app in Start, and then click **Uninstall**.

  -or-

- Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.BingSports"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}**

  -and-

- Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.BingSports | Remove-AppxPackage**

To remove the Twitter app:

- Right-click the app in Start, and then click **Uninstall**.

  -or-

- Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online |**

Where-Object {$_.PackageName -Like "*.Twitter"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}

-and-

- Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage *.Twitter | Remove-AppxPackage**

To remove the XBOX app:

- Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.XboxApp"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}**

  -and-

- Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.XboxApp | Remove-AppxPackage**

To remove the Sway app:

- Right-click the app in Start, and then click **Uninstall**.

  -or-

- Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.Office.Sway"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}**

  -and-

- Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.Office.Sway | Remove-AppxPackage**

To remove the OneNote app:

- Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.Office.OneNote"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}**

  -and-

- Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.Office.OneNote | Remove-AppxPackage**

To remove the Get Office app:

- Right-click the app in Start, and then click **Uninstall**.

  -or-

- Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.MicrosoftOfficeHub"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}**

  -and-

- Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.MicrosoftOfficeHub | Remove-AppxPackage**

To remove the Get Skype app:

- Right-click the Sports app in Start, and then click **Uninstall**.

  -or-

- Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.SkypeApp"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}**

  -and-

- Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.SkypeApp | Remove-AppxPackage**

To remove the Sticky notes app:

- Remove the app for new user accounts. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxProvisionedPackage -Online | Where-Object {$_.PackageName -Like "Microsoft.MicrosoftStickyNotes"} | ForEach-Object { Remove-AppxProvisionedPackage -Online -PackageName $_.PackageName}**

  -and-

- Remove the app for the current user. From an elevated command prompt, run the following Windows PowerShell command: **Get-AppxPackage Microsoft.MicrosoftStickyNotes | Remove-AppxPackage**

18. Settings > Privacy & security

Use Settings > Privacy & security to configure some settings that may be important to your organization. Except for the Feedback & Diagnostics page, these settings must be configured for every user account that signs into the PC.

18.1 General

General includes options that don't fall into other areas.

Windows 10, version 1703 options

To turn off **Let apps use advertising ID to make ads more interesting to you based on your app usage (turning this off will reset your ID)**:

- Turn off the feature in the UI.

  Note

  When you turn this feature off in the UI, it turns off the advertising ID, not just resets it.

  -or-

- **Enable** the Group Policy: **Computer Configuration** > **Administrative Templates** > **System** > **User Profiles** > **Turn off the advertising ID**.

  -or-

- Create a REG_DWORD registry setting named **Enabled** in **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AdvertisingInfo** with a value of 0 (zero).

  -and-

- Create a REG_DWORD registry setting named **DisabledByGroupPolicy** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AdvertisingInfo** with a value of 1 (one).

To turn off **Let websites provide locally relevant content by accessing my language list**:

- Turn off the feature in the UI.

  -or-

- Create a new REG_DWORD registry setting named **HttpAcceptLanguageOptOut** in **HKEY_CURRENT_USER\Control Panel\International\User Profile** with a value of 1.

To turn off **Let Windows track app launches to improve Start and search results**:

- Turn off the feature in the UI.

  -or-

- Create a REG_DWORD registry setting named **Start_TrackProgs** in **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced** with value of 0 (zero).

Windows Server 2016 and Windows 10, version 1607 and earlier options

To turn off **Let apps use my advertising ID for experiences across apps (turning this off will reset your ID)**:

- Turn off the feature in the UI.

  Note

  When you turn this feature off in the UI, it turns off the advertising ID, not just resets it.

  -or-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > System > User Profiles > Turn off the advertising ID**.

-or-

- Create a REG_DWORD registry setting named **Enabled** in **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AdvertisingInfo** with a value of 0 (zero).

-or-

- Create a REG_DWORD registry setting named **DisabledByGroupPolicy** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Advertising Info** with a value of 1 (one).

To turn off **Turn on Microsoft Defender SmartScreen to check web content (URLs) that Microsoft Store apps use**:

- Turn off the feature in the UI.

  -or-

- Create a REG_DWORD registry setting named **EnableWebContentEvaluation** in **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\App Host** with a value of 0 (zero).

To turn off **Send Microsoft info about how I write to help us improve typing and writing in the future**:

Note

If the diagnostic data level is set to either **Basic** or **Security**, this is turned off automatically.

- Turn off the feature in the UI.

To turn off **Let websites provide locally relevant content by accessing my language list**:

- Turn off the feature in the UI.

  -or-

- Create a new REG_DWORD registry setting named **HttpAcceptLanguageOptOut** in **HKEY_CURRENT_USER\Control Panel\International\User Profile** with a value of 1.

To turn off **Let apps on my other devices open apps and continue experiences on this device**:

- Turn off the feature in the UI.

  -or-

- Disable the Group Policy: **Computer Configuration > Administrative Templates > System > Group Policy > Continue experiences on this device**.

  -or-

- Create a REG_DWORD registry setting named **EnableCdp** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System** with a value of 0 (zero).

To turn off **Let apps on my other devices use Bluetooth to open apps and continue experiences on this device**:

- Turn off the feature in the UI.

18.2 Location

In the **Location** area, you choose whether devices have access to location-specific sensors and which apps have access to the device's location.

To turn off **Location for this device**:

- Click the **Change** button in the UI.

  -or-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Location and Sensors > Turn off location**.

  -or-

- Create a REG_DWORD registry setting named **DisableLocation** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\LocationAndSensors** with a value of 1 (one).

To turn off **Allow apps to access your location**:

- Turn off the feature in the UI.

  -or-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access location** and set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessLocation** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a **value of 2 (two)**.

To turn off **Location history**:

- Erase the history using the **Clear** button in the UI.

To turn off **Choose apps that can use your location**:

- Turn off each app using the UI.

18.3 Camera

In the **Camera** area, you can choose which apps can access a device's camera.

To turn off **Let apps use my camera**:

- Turn off the feature in the UI.

  -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access the camera**
  - Set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessCamera** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a value of 2 (two).

To turn off **Choose apps that can use your camera**:

- Turn off the feature in the UI for each app.

18.4 Microphone

In the **Microphone** area, you can choose which apps can access a device's microphone.

To turn off **Let apps use my microphone**:

- Turn off the feature in the UI.

  -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access the microphone**
  - Set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessMicrophone** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a value of 2 (two)

To turn off **Choose apps that can use your microphone**:

- Turn off the feature in the UI for each app.

18.5 Notifications

To turn off notifications network usage:

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Start Menu and Taskbar > Notifications > Turn off Notifications network usage**

  -or-

- Create a REG_DWORD registry setting named **NoCloudApplicationNotification** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\PushNotifications** with a value of 1 (one)

In the **Notifications** area, you can also choose which apps have access to notifications.

To turn off **Let apps access my notifications**:

- Turn off the feature in the UI.

  -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access notifications**
  - Set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessNotifications** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a value of 2 (two)

18.6 Speech

In the **Speech** area, you can configure the functionality as such:

To turn off dictation of your voice, speaking to Cortana and other apps, and to prevent sending your voice input to Microsoft Speech services:

- Toggle the Settings -> Privacy -> Speech -> **Online speech recognition** switch to **Off**

  -or-

- **Disable** the Group Policy: **Computer Configuration > Administrative Templates > Control Panel > Regional and Language Options > Allow users to enable online speech recognition services**

  -or-

- Create a REG_DWORD registry setting named **HasAccepted** in **HKEY_CURRENT_USER\Software\Microsoft\Speech_OneCore\Settings\OnlineSpeechPrivacy** with a **value of 0 (zero)**

If you're running at Windows 10, version 1703 up to and including Windows 10, version 1803, you can turn off updates to the speech recognition and speech synthesis models:

- **Disable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Speech > Allow automatic update of Speech Data**

  -or-

- Create a REG_DWORD registry setting named **AllowSpeechModelUpdate** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Speech** with a **value of 0 (zero)**

18.7 Account info

In the **Account Info** area, you can choose which apps can access your name, picture, and other account info.

To turn off **Let apps access my name, picture, and other account info**:

- Turn off the feature in the UI.

  -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access account information**
  - Set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessAccountInfo** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppPrivacy** with a **value of 2 (two)**.

To turn off **Choose the apps that can access your account info**:

- Turn off the feature in the UI for each app.

18.8 Contacts

In the **Contacts** area, you can choose which apps can access an employee's contacts list.

To turn off **Choose apps that can access contacts**:

- Turn off the feature in the UI for each app.

  -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access contacts**
  - Set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessContacts** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppPrivacy** with a value of 2 (two).

18.9 Calendar

In the **Calendar** area, you can choose which apps have access to an employee's calendar.

To turn off **Let apps access my calendar**:

- Turn off the feature in the UI.

  -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access the calendar**. Set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessCalendar** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppPrivacy** with a value of 2 (two).

To turn off **Choose apps that can access calendar**:

- Turn off the feature in the UI for each app.

18.10 Call history

In the **Call history** area, you can choose which apps have access to an employee's call history.

To turn off **Let apps access my call history**:

- Turn off the feature in the UI.

  -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access call history**
  - Set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessCallHistory** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a value of 2 (two).

18.11 Email

In the **Email** area, you can choose which apps have access and can send email.

To turn off **Let apps access and send email**:

- Turn off the feature in the UI.

  -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access email**
    - Set the **Select a setting** box to **Force Deny**.

    -or-

- Create a REG_DWORD registry setting named **LetAppsAccessEmail** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a value of 2 (two).

18.12 Messaging

In the **Messaging** area, you can choose which apps can read or send messages.

To turn off **Let apps read or send messages (text or MMS)**:

- Turn off the feature in the UI.

    -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access messaging**
    - Set the **Select a setting** box to **Force Deny**.

    -or-

- Create a REG_DWORD registry setting named **LetAppsAccessMessaging** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a value of 2 (two).

To turn off **Choose apps that can read or send messages**:

- Turn off the feature in the UI for each app.

To turn off Message Sync

- Create a REG_DWORD registry setting named **AllowMessageSync** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Messaging** and set the **value to 0 (zero)**.

    -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Messaging**
    - Set the **Allow Message Service Cloud Sync** to **Disable**.

18.13 Phone calls

In the **Phone calls** area, you can choose which apps can make phone calls.

To turn off **Let apps make phone calls**:

- Turn off the feature in the UI.

  -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps make phone calls** and set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessPhone** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a value of 2 (two).

To turn off **Choose apps that can make phone calls**:

- Turn off the feature in the UI for each app.

18.14 Radios

In the **Radios** area, you can choose which apps can turn a device's radio on or off.

To turn off **Let apps control radios**:

- Turn off the feature in the UI.

  -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps control radios** and set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessRadios** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a value of 2 (two).

To turn off **Choose apps that can control radios**:

- Turn off the feature in the UI for each app.

18.15 Other devices

In the **Other Devices** area, you can choose whether devices that aren't paired to PCs, such as an Xbox One, can share and sync info.

To turn off **Let apps automatically share and sync info with wireless devices that don't explicitly pair with your PC, tablet, or phone**:

- Turn off the feature in the UI by going to Settings > Privacy & security > Other devices > "Communicate with unpaired devices. Let apps automatically share and sync info with

wireless devices that don't explicitly pair with your PC, tablet, or phone" and **Turn it OFF**.

-or-

- **Enable** the Group Policy: **Computer Configuration** > **Administrative Templates** > **Windows Components** > **App Privacy** > **Let Windows apps communicate with unpaired devices** and set the **Select a setting** box to **Force Deny**.

-or-

- Create a REG_DWORD registry setting named **LetAppsSyncWithDevices** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a **value of 2 (two)**.

To turn off **Let your apps use your trusted devices (hardware you've already connected, or comes with your PC, tablet, or phone)**:

- Turn off the feature in the UI.

-or-

- **Enable** the Group Policy: **Computer Configuration** > **Administrative Templates** > **Windows Components** > **App Privacy** > **Let Windows apps access trusted devices** and set the **Select a setting** box to **Force Deny**.

-or-

- Create a REG_DWORD registry setting named **LetAppsAccessTrustedDevices** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a **value of 2 (two)**.

18.16 Feedback & diagnostics

In the **Feedback & Diagnostics** area, you can choose how often you're asked for feedback and how much diagnostic and usage information is sent to Microsoft. If you're looking for content on what each diagnostic data level means and how to configure it in your organization, see Configure Windows diagnostic data in your organization.

Note

Feedback frequency only applies to user-generated feedback, not diagnostic and usage data sent from the device.

To change how frequently **Windows should ask for my feedback**:

- To change from **Automatically (Recommended)**, use the drop-down list in the UI.

-or-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds > Do not show feedback notifications**

  -or-

- Create a REG_DWORD registry setting named **DoNotShowFeedbackNotifications** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DataCollection** with a value of 1 (one).

  -or-

- Create the registry keys (REG_DWORD type):
  - HKEY_CURRENT_USER\Software\Microsoft\Siuf\Rules\PeriodInNanoSeconds
  - HKEY_CURRENT_USER\Software\Microsoft\Siuf\Rules\NumberOfSIUFInPeriod

    Based on these settings:

Setting	PeriodInNanoSeconds	NumberOfSIUFInPeriod
Automatically	Delete the registry setting	Delete the registry setting
Never	0	0
Always	100000000	Delete the registry setting
Once a day	864000000000	1
Once a week	6048000000000	1

To change the level of diagnostic and usage data sent when you **Send your device data to Microsoft**:

- Click either the **Required (Basic)** or **Optional (Full)** options.

  -or-

- **Enable** the Group Policy: **Computer Configuration\Administrative Templates\Windows Components\Data Collection And Preview Builds\Allow Telemetry** and **set it to a value of 0**.

  -or-

- Create a REG_DWORD registry setting in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DataCollection\AllowTelemetry** with a **value of 0**.

Note

If the **Security** option is configured by using Group Policy or the Registry, the value will not be reflected in the UI. The **Security** option is only available in Windows 10 and Windows 11 Enterprise edition.

To turn off tailored experiences with relevant tips and recommendations by using your diagnostics data:

- Turn off the feature in the UI.

  -or-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Cloud Content > Turn off Microsoft consumer experiences**

  -or-

- Create a REG_DWORD registry setting named **DisableWindowsConsumerFeatures** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent** with a value of **1**

  -and-

- **Enable** the Group Policy: **User Configuration > Administrative Templates > Windows Components > Cloud Content > Do not use diagnostic data for tailored experiences**

  -or-

- Create a REG_DWORD registry setting named **DisableTailoredExperiencesWithDiagnosticData** in **HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\CloudContent** with a **value of 1 (one)**

18.17 Background apps

In the **Background Apps** area, you can choose which apps can run in the background.

To turn off **Let apps run in the background**:

- In the **Background apps** settings page, set **Let apps run in the background** to **Off**.

  -or-

- In the **Background apps** settings page, turn off the feature for each app.

-or-

- **Enable** the Group Policy (only applicable for Windows 10 version 1703 and above and Windows 11): **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps run in the background** and set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsRunInBackground** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a **value of 2 (two)**

Note

Some apps, including Cortana and Search, might not function as expected if you set **Let apps run in the background** to **Force Deny**.

18.18 Motion

In the **Motion** area, you can choose which apps have access to your motion data.

To turn off **Let Windows and your apps use your motion data and collect motion history**:

- Turn off the feature in the UI.

  -or-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access motion** and set the **Default for all apps** to **Force Deny**

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessMotion** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a **value of 2 (two)**.

18.19 Tasks

In the **Tasks** area, you can choose which apps have access to your tasks.

To turn this off:

- Turn off the feature in the UI.

  -or-

- Apply the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy > Let Windows apps access Tasks**. Set the **Select a setting** box to **Force Deny**.

  -or-

- Create a REG_DWORD registry setting named **LetAppsAccessTasks** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a **value of 2 (two)**.

18.20 App Diagnostics

In the **App diagnostics** area, you can choose which apps have access to your diagnostic information.

To turn this off:

- Turn off the feature in the UI.

-or-

- **Enable** the Group Policy: **Computer Configuration** > **Administrative Templates** > **Windows Components** > **App Privacy** > **Let Windows apps access diagnostic information about other apps**

  -or-

- Create a REG_DWORD registry setting named **LetAppsGetDiagnosticInfo** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a **value of 2 (two)**.

18.21 Inking & Typing

In the **Inking & Typing** area you can configure the functionality as such:

To turn off Inking & Typing data collection:

- In the UI go to **Settings -> Privacy -> Diagnostics & Feedback -> Improve inking and typing** and turn it to **Off**

  -OR-

  Disable the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Text Input > Improve inking and typing recognition**

  -and-

  Disable the Group Policy: **User Configuration > Administrative Templates > Control Panel > Regional and Language Options > Handwriting personalization > Turn off automatic learning**

  -OR-

- Set **RestrictImplicitTextCollection** registry REG_DWORD setting in **HKEY_CURRENT_USER\Software\Microsoft\InputPersonalization** to a **value of 1 (one)**

  -and-

- Set **RestrictImplicitInkCollection** registry REG_DWORD setting in **HKEY_CURRENT_USER\Software\Microsoft\InputPersonalization** to a **value of 1 (one)**

18.22 Activity History

In the **Activity History** area, you can choose turn Off tracking of your Activity History.

To turn this Off in the UI:

- Turn **Off** the feature in the UI by going to Settings -> Privacy -> Activity History and **un-checking** the **Store my activity history on this device** AND **unchecking** the **Send my activity History to Microsoft** checkboxes

-OR-

- **Disable** the Group Policy: **Computer Configuration > Administrative Templates > System > OS Policies** named **Enables Activity Feed**

  -and-

- **Disable** the Group Policy: **Computer Configuration > Administrative Templates > System > OS Policies** named **Allow publishing of User Activities**

  -and-

- **Disable** the Group Policy: **Computer Configuration > Administrative Templates > System > OS Policies >** named **Allow upload of User Activities**

-OR-

- Create a REG_DWORD registry setting named **EnableActivityFeed** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System** with a **value of 0 (zero)**

  -and-

- Create a REG_DWORD registry setting named **PublishUserActivities** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System** with a **value of 0 (zero)**

  -and-

- Create a REG_DWORD registry setting named **UploadUserActivities** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System** with a **value of 0 (zero)**

18.23 Voice Activation

In the **Voice activation** area, you can choose turn Off apps ability to listen for a Voice keyword.

To turn this Off in the UI:

- Turn **Off** the feature in the UI by going to **Settings -> Privacy -> Voice activation** and toggle **Off** the **Allow apps to use voice activation** AND also toggle **Off** the **Allow apps to use voice activation when this device is locked**

-OR-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy >** named **Let Windows apps activate with voice** and set the **Select a setting** box to **Force Deny**

-and-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > App Privacy >** named **Let Windows apps activate with voice while the system is locked** box to **Force Deny**

-OR-

- Create a REG_DWORD registry setting named **LetAppsActivateWithVoice** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a **value of 2 (two)**

  -and-

- Create a REG_DWORD registry setting named **LetAppsActivateWithVoiceAboveLock** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy** with a **value of 2 (two)**

18.24 News and interests

In the **Windows Feeds** area, you can choose which apps have access to your diagnostic information.

To turn this off:

- Create a REG_DWORD registry setting named **EnableFeeds** in **HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows Feeds** with a **value of 0 (zero)**.

19. Software Protection Platform

Enterprise customers can manage their Windows activation status with volume licensing using an on-premises Key Management Server. You can opt out of sending KMS client activation data to Microsoft automatically by doing one of the following:

For Windows 10 and Windows 11:

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Software Protection Platform > Turn off KMS Client Online AVS Validation**

  -or-

- Create a REG_DWORD registry setting named **NoGenTicket** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\CurrentVersion\Software Protection Platform** with a **value of 1 (one)**.

For Windows Server 2019 or later:

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Software Protection Platform > Turn off KMS Client Online AVS Validation**

-or-

- Create a REG_DWORD registry setting named **NoGenTicket** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\CurrentVersion\Software Protection Platform** with a value of 1 (one).

For Windows Server 2016:

- Create a REG_DWORD registry setting named **NoAcquireGT** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\CurrentVersion\Software Protection Platform** with a **value of 1 (one)**.

Note

Due to a known issue the **Turn off KMS Client Online AVS Validation** group policy does not work as intended on Windows Server 2016; the **NoAcquireGT** value needs to be set instead. The Windows activation status will be valid for a rolling period of 180 days with weekly activation status checks to the KMS.

20. Storage health

Enterprise customers can manage updates to the Disk Failure Prediction Model.

For Windows 10 and Windows 11:

- **Disable** this Group Policy: **Computer Configuration > Administrative Templates > System > Storage Health > Allow downloading updates to the Disk Failure Prediction Model**

  -or-

- Create a REG_DWORD registry setting named **AllowDiskHealthModelUpdates** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\StorageHealth** with a **value of 0**.

21. Sync your settings

You can control if your settings are synchronized:

- In the UI: **Settings > Accounts > Sync your settings**

  -or-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Sync your settings > Do not sync**. Leave the "Allow users to turn syncing on" checkbox **unchecked**.

  -or-

- Create a REG_DWORD registry setting named **DisableSettingSync** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\SettingSync** with a value of 2 (two) and another named **DisableSettingSyncUserOverride** in

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\SettingSync with a value of 1 (one).

To turn off Messaging cloud sync:

- Create a REG_DWORD registry setting named **CloudServiceSyncEnabled** in **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Messaging** and set to a **value of 0 (zero)**.

  Note

  There is no Group Policy corresponding to this registry key.

22. Teredo

You can disable Teredo by using Group Policy or by using the netsh.exe command. For more info on Teredo, see Internet Protocol Version 6, Teredo, and Related Technologies.

Note

If you disable Teredo, some XBOX gaming features and Delivery Optimization (with Group or Internet peering) will not work.

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Network > TCPIP Settings > IPv6 Transition Technologies > Set Teredo State** and set it to **Disabled State**.

  -or-

- Create a new REG_SZ registry setting named **Teredo_State** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\TCPIP\v6Transition** with a value of **Disabled**.

23. Wi-Fi Sense

Important

Beginning with Windows 10, version 1803, Wi-Fi Sense is no longer available. The following section only applies to Windows 10, version 1709 and prior. Please see Connecting to open Wi-Fi hotspots in Windows 10 for more details.

Wi-Fi Sense automatically connects devices to known hotspots and to the wireless networks the person's contacts have shared with them.

To turn off **Connect to suggested open hotspots** and **Connect to networks shared by my contacts**:

- Turn off the feature in the UI in Settings > Network & Internet > Wi-Fi

  -or-

- **Disable** the Group Policy: **Computer Configuration > Administrative Templates > Network > WLAN Service > WLAN Settings > Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services**.

  -or-

- Create a new REG_DWORD registry setting named **AutoConnectAllowedOEM** in **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WcmSvc\wifinetworkmanager\config** with a **value of 0 (zero)**.

When turned off, the Wi-Fi Sense settings still appear on the Wi-Fi Settings screen, but they're non-functional and they can't be controlled by the employee.

24. Microsoft Defender Antivirus

You can disconnect from the Microsoft Antimalware Protection Service.

Important

Required Steps BEFORE setting the Microsoft Defender Antivirus Group Policy or RegKey on Windows 10 version 1903

1. Ensure Windows and Microsoft Defender Antivirus are fully up to date.
2. Search the Start menu for "Tamper Protection" by clicking on the search icon next to the Windows Start button. Then scroll down to the Tamper Protection toggle and turn it **Off**. This will allow you to modify the Registry key and allow the Group Policy to make the setting. Alternatively, you can go to **Windows Security Settings -> Virus & threat protection, click on Manage Settings** link and then scroll down to the Tamper Protection toggle to set it to **Off**.

- **Enable** the Group Policy **Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > MAPS > Join Microsoft MAPS** and then select **Disabled** from the drop-down box named **Join Microsoft MAPS**

-OR-

- Use the registry to set the REG_DWORD value **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Spynet\SpyNetReporting** to **0 (zero)**.

  -and-

- Delete the registry setting **named** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Updates**.

You can stop sending file samples back to Microsoft.

- **Enable** the Group Policy **Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > MAPS > Send file samples when further analysis is required** to **Never Send**.

-or-

- Use the registry to set the REG_DWORD value **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Spynet\SubmitSamplesConsent** to **2 (two) for Never Send**.

You can stop downloading **Definition Updates**:

Note

The Group Policy path for 1809 and earlier builds is **Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > Signature Updates**

- **Enable** the Group Policy **Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > Security Intelligence Updates > Define the order of sources for downloading definition updates** and set it to **FileShares**.

  -and-

- **Disable** the Group Policy **Computer Configuration > Administrative Templates > Windows Components > Microsoft Defender Antivirus > Security Intelligence Updates > Define file shares for downloading definition updates** and set it to **Nothing**.

  -or-

- Create a new REG_SZ registry setting named **FallbackOrder** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Signature Updates** with a value of **FileShares**.

  -and-

- **Remove** the **DefinitionUpdateFileSharesSources** reg value if it exists under **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Signature Updates**

You can turn off **Malicious Software Reporting Tool (MSRT) diagnostic data**:

- Set the REG_DWORD value **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MRT\DontReportInfectionInformation** to **1**.

  Note

  There is no Group Policy to turn off the Malicious Software Reporting Tool diagnostic data.

You can turn off **Enhanced Notifications** as follows:

- Set in the UI: Settings -> Update & Security -> Windows Security -> Virus & Threat Protection -> Virus & Threat Protection Manage Settings -> scroll to bottom for

Notifications, click Change Notifications Settings -> Notifications -> click Manage Notifications -> Turn off General Notifications

-or-

- **Enable** the Group Policy **Turn off enhanced notifications** under **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Microsoft Defender Antivirus** > **Reporting**.

-or-

- Create a new REG_DWORD registry setting named **DisableEnhancedNotifications** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Reporting** and enter the decimal value **1**.

24.1 Microsoft Defender SmartScreen

To disable Microsoft Defender SmartScreen:

In Group Policy, configure:

- **Computer Configuration > Administrative Templates > Windows Components > Windows Defender SmartScreen > Explorer > Configure Windows Defender SmartScreen** to be **Disabled**

-and-

- **Computer Configuration > Administrative Templates > Windows Components > File Explorer > Configure Windows Defender SmartScreen** : **Disable**

-and-

- **Computer Configuration > Administrative Templates > Windows Components > Windows Defender SmartScreen > Explorer > Configure app install control** : **Enable**, and select **Turn off app recommendations**

-OR-

- Create a REG_DWORD registry setting named **EnableSmartScreen** in **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System** with a **value of 0 (zero)**.

-and-

- Create a REG_DWORD registry setting named **ConfigureAppInstallControlEnabled** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\SmartScreen** with a **value of 1**.

-and-

- Create an SZ registry setting named **ConfigureAppInstallControl** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\SmartScreen** with a value of **Anywhere**.

25. Personalized Experiences

Personalized experiences provides features such as different background images and text on the lock screen, suggested apps, Microsoft account notifications, and Windows tips. Example features include Windows Spotlight and Start Suggestions. You can control them by using the Group Policy.

Note

This excludes how individual experiences (e.g., Windows Spotlight) can be controlled by users in Windows Settings.

If you're running Windows 10, version 1607 or later, or Windows 11, you need to:

- **Enable** the following Group Policy **User Configuration > Administrative Templates > Windows Components > Cloud Content > Turn off all Windows spotlight features**

  -or-

- Create a new REG_DWORD registry setting named **DisableWindowsSpotlightFeatures** in **HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\CloudContent** with a **value of 1 (one)**.

-AND-

- Enable the following Group Policy **Computer Configuration > Administrative Templates > Windows Components > Cloud Content > Turn off cloud optimized content**

  -or-

- Create a new REG_DWORD registry setting named **DisableCloudOptimizedContent** in **HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\CloudContent** with a **value of 1 (one)**.

  Note

  This must be done within 15 minutes after Windows 10 or Windows 11 is installed. Alternatively, you can create an image with this setting.

26. Microsoft Store

You can turn off the ability to launch apps from the Microsoft Store that were preinstalled or downloaded. This will also turn off automatic app updates, and the Microsoft Store will be disabled. In addition, new email accounts cannot be created by clicking **Settings > Accounts > Email & app accounts > Add an account**. On Windows Server 2016, this will block Microsoft Store calls from Universal Windows Apps.

- **Disable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Store > Disable all apps from Microsoft Store**.

  -or-

- Create a new REG_DWORD registry setting named **DisableStoreApps** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore** with a value of 1 (one).

-AND-

- **Enable** the Group Policy: **Computer Configuration > Administrative Templates > Windows Components > Store > Turn off Automatic Download and Install of updates**.

  -or-

- Create a new REG_DWORD registry setting named **AutoDownload** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore** with a value of 2 (two).

27. Apps for websites

You can turn off apps for websites, preventing customers who visit websites that are registered with their associated app from directly launching the app.

- **Disable** the Group Policy: **Computer Configuration > Administrative Templates > System > Group Policy > Configure web-to-app linking with URI handlers**

  -or-

- Create a new REG_DWORD registry setting named **EnableAppUriHandlers** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System** with a **value of 0 (zero)**.

28. Delivery Optimization

Delivery Optimization is the downloader of Windows updates, Microsoft Store apps, Office and other content from Microsoft. Delivery Optimization can also download from sources in addition to Microsoft, which not only helps when you have a limited or unreliable Internet connection, but can also help you reduce the amount of bandwidth needed to keep all of your organization's PCs up-to-date. If you have Delivery Optimization Peer-to-Peer option turned on, PCs on your network may send and receive updates and apps to other PCs on your local network, if you choose, or to PCs on the Internet.

By default, PCs running Windows 10 or Windows 11 will only use Delivery Optimization to get and receive updates for PCs and apps on your local network.

Use the UI, Group Policy, or Registry Keys to set up Delivery Optimization.

In Windows 10, version 1607 and above, and Windows 11 you can stop network traffic related to Delivery Optimization Cloud Service by setting **Download Mode** to **Simple Mode** (99), as described below.

28.1 Settings > Update & security

You can set up Delivery Optimization Peer-to-Peer from the **Settings** UI.

- Go to **Settings > Update & security > Windows Update > Advanced options > Choose how updates are delivered**.

28.2 Delivery Optimization Group Policies

You can find the Delivery Optimization Group Policy objects under **Computer Configuration > Administrative Templates > Windows Components > Delivery Optimization**.

Policy	Description
Download Mode	Lets you choose where Delivery Optimization gets or sends updates and apps, including • **None**. Turns off Delivery Optimization. • **Group**. Gets or sends updates and apps to PCs on the same local network domain. • **Internet**. Gets or sends updates and apps to PCs on the Internet. • **LAN**. Gets or sends updates and apps to PCs on the same NAT only. • **Simple**. Simple download mode with no peering. • **Bypass**. Use BITS instead of Windows Update Delivery Optimization. **Set to Bypass** to restrict traffic.
Group ID	Lets you provide a Group ID that limits which PCs can share apps and updates. **Note:** This ID must be a GUID.
Max Cache Age	Lets you specify the maximum time (in seconds) that a file is held in the Delivery Optimization cache. The default value is 259200 seconds (3 days).
Max Cache Size	Lets you specify the maximum cache size as a percentage of disk size. The default value is 20, which represents 20% of the disk.
Max Upload Bandwidth	Lets you specify the maximum upload bandwidth (in KB/second) that a device uses across all concurrent upload activity. The default value is 0, which means unlimited possible bandwidth.

For a comprehensive list of Delivery Optimization Policies, see Delivery Optimization Reference.

28.3 Delivery Optimization

- **Enable** the **Download Mode** Group Policy under **Computer Configuration > Administrative Templates > Windows Components > Delivery Optimization** and set the **Download Mode** to **"Simple Mode (99)"** to prevent traffic between peers as well as traffic back to the Delivery Optimization Cloud Service.

-or-

- Create a new REG_DWORD registry setting named **DODownloadMode** in **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization** to a value of **99 (Ninety-nine)**.

For more info about Delivery Optimization in general, see Windows Update Delivery Optimization: FAQ.

For IT Professionals, information about Delivery Optimization is available here: Delivery Optimization for Windows 10 updates.

29. Windows Update

You can turn off Windows Update by setting the following registry entries:

- Add a REG_DWORD value named **DoNotConnectToWindowsUpdateInternetLocations** to **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate** and set the value to 1.

  -and-

- Add a REG_DWORD value named **DisableWindowsUpdateAccess** to **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate** and set the value to 1.

  -and-

- Add a REG_SZ value named **WUServer** to **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate** and ensure it is blank with a space character **" "**.

  -and-

- Add a REG_SZ value named **WUStatusServer** to **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate** and ensure it is blank with a space character **" "**.

  -and-

- Add a REG_SZ value named **UpdateServiceUrlAlternate** to **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate** and ensure it is blank with a space character **" "**.

  -and-

- Add a REG_DWORD value named **UseWUServer** to **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU** and set the **value to 1 (one)**.

-OR-

- Set the Group Policy **Computer Configuration > Administrative Templates > Windows Components > Windows Update > Do not connect to any Windows Update Internet locations** to **Enabled**

  -and-

- Set the Group Policy **Computer Configuration > Administrative Templates > System > Internet Communication Management > Internet Communication Settings > Turn off access to all Windows Update features** to **Enabled**

  -and-

- Set the Group Policy **Computer Configuration > Administrative Templates > Windows Components > Windows Update > Specify intranet Microsoft update service location** to **Enabled** and ensure all Option settings (Intranet Update Service, Intranet Statistics Server, Alternate Download Server) are set to **" "**

  -and-

- Set the Group Policy **User Configuration > Administrative Templates > Windows Components > Windows Update > Remove access to use all Windows Update features** to **Enabled** and then set **Computer Configurations** to **0 (zero)**.

You can turn off automatic updates by doing the following. This is not recommended.

- Add a REG_DWORD value named **AutoDownload** to **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\WindowsStore\WindowsUpdate** and set the value to 5.

For China releases of Windows 10 there is one additional Regkey to be set to prevent traffic:

- Add a REG_DWORD value named **HapDownloadEnabled** to **HKEY_LOCAL_MACHINE\Software\Microsoft\LexiconUpdate\loc_0804** and set the **value to 0 (zero)**.

30. Cloud Clipboard

Specifies whether clipboard items roam across devices. When this is allowed, an item copied to the clipboard is uploaded to the cloud so that other devices can access it. Clipboard items in the cloud can be downloaded and pasted across your Windows 10 and Windows 11 devices.

Most restricted value is 0.

ADMX Info:

- GP Friendly name: Allow Clipboard synchronization across devices
- GP name: AllowCrossDeviceClipboard
- GP path: System/OS Policies
- GP ADMX file name: OSPolicy.admx

The following list shows the supported values:

- 0 – Not allowed
- 1 (default) – Allowed

31. Services Configuration

Services Configuration is used by Windows components and apps, such as the telemetry service, to dynamically update their configuration. If you turn off this service, apps using this service may stop working.

You can turn off Services Configuration by setting the following registry entries:

Add a REG_DWORD value named **DisableOneSettingsDownloads** to **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DataCollection** and set the value to **1**.

32. Widgets

Widgets is a news and feeds service that can be customized by the user. If you turn off this service, apps using this service may stop working.

You can turn off Widgets by setting the following registry entries:

Add a REG_DWORD value named **AllowWidgets** to **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Widgets** and set the value to **0**.

Allowed traffic list for Windows Restricted Traffic Limited Functionality Baseline

Allowed traffic endpoints

activation-v2.sls.microsoft.com/*

crl.microsoft.com/pki/crl/*

ocsp.digicert.com/*

www.microsoft.com/pkiops/*

To learn more, see Device update management and Configure Automatic Updates by using Group Policy.

Recommended content

- **Configure Windows diagnostic data in your organization (Windows 10 and Windows 11) - Windows Privacy**

Use this article to make informed decisions about how you can configure Windows diagnostic data in your organization.

- **Windows 10, version 21H1, connection endpoints for non-Enterprise editions - Windows Privacy**

  Explains what Windows 10 endpoints are used in non-Enterprise editions. Specific to Windows 10, version 21H1.

- **Connection endpoints for Windows 10 Enterprise, version 2004 - Windows Privacy**

  Explains what Windows 10 endpoints are used for, how to turn off traffic to them, and the impact. Specific to Windows 10 Enterprise, version 2004.

- **Windows 10, version 21H2, Windows 10, version 21H1, Windows 10, version 20H2 and Windows 10, version 2004 required diagnostic events and fields (Windows 10) - Windows Privacy**

  Learn more about the required Windows 10 diagnostic data gathered.

- **Group policy settings - Configuration Manager**

  Understand the local and group policy settings in Windows used by Configuration Manager and Desktop Analytics

- **Windows 10, version 1909, connection endpoints for non-Enterprise editions - Windows Privacy**

  Explains what Windows 10 endpoints are used in non-Enterprise editions. Specific to Windows 10, version 1909.

- **Windows 11 - release information**

  Learn release information for Windows 11 releases

- **Resolved issues in Windows 11**

  Resolved issues in Windows 11