Windows 11 policy settings

Article • 05/02/2023

The following table lists the Windows 11 policy settings used in Microsoft Managed Desktop.

ControlPanelDisplay.admx

- Location: Machine
- Policy path: `Control Panel\Personalization`
- Polity setting name: Prevent lock screen background
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\Personalization!AnimateLockScreenBackground`
- Supported on: At least Windows 10
- Setting value: -

This policy setting controls whether the lock screen image is static or has a subtle panning effect driven by the device's accelerometer output.

- If you turn on this setting, motion is prevented and the user sees the traditional static lock screen background image.
- If you turn off this setting (and the device has an accelerometer), the user sees the lock screen background pan around a still image as they physically move their device.

Globalization.admx

- Location: Machine
- Policy path: `Control Panel\Regional and Language Options`
- Policy setting name: Restrict Language Pack and Language Feature Installation
- Registry information: `HKLM\Software\Policies\Microsoft\Control Panel\International!RestrictLanguagePacksAndFeaturesInstall`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

This policy setting restricts all users from installing language packs and language features on demand packages. This policy doesn't restrict switching the Windows language if you want to restrict the Windows language use the **Restricts the UI languages Windows uses for all logged users** policy.

- If you turn on this policy setting, users can't install language packs and language features.
- If you turn off or don't configure this policy setting, users can install language packs or features.

SecGuide.admx

- Location: Machine
- Policy path: `MS Security Guide`
- Policy setting name: Limits print driver installation to Administrators
- Registry information: `HKLM\Software\Policies\Microsoft\Windows NT\Printers\PointAndPrint!RestrictDriverInstallationToAdministrators`
- Supported on: At least Windows Server 2008 R2 or Windows 7
- Setting value: -

Determines whether users that aren't an Administrator can install printer drivers on this computer. By default, users that aren't Administrators can't install print drivers on this computer.

- If you turn on this setting or don't configure it, the system limits installation of print drivers to Administrators of this computer.
- If you turn off this setting, the system doesn't limit the installation of print drivers to this computer. For more information, see Restrict installation of new printer .

DnsClient.admx

- Location: Machine
- Policy path: `Network\DNS Client`
- Policy setting name: Configure DNS over HTTPS (DoH) name resolution
- Registry information: `HKLM\Software\Policies\Microsoft\Windows NT\DNSClient!DoHPolicy`
- Supported on: At least Windows Vista
- Setting value: -

Specifies if the DNS client will perform name resolution over DNS over HTTPS (DoH). By default, the DNS client will do classic DNS name resolution (over UDP or TCP). This setting can enhance the DNS client to use DoH protocol to resolve domain names.

To use this policy setting, select **Enabled** and then select one of the following options from the dropdown menu:

- **Prohibit DoH**: No DoH name resolution is performed.
- **Allow DoH**: Perform DoH queries if the configured DNS servers support it. If they don't support, it tries the classic name resolution.
- **Require DoH**: Allow only DoH name resolution. If there are no DoH-capable DNS servers configured, the name resolution fails.

If you turn off this policy setting or if you don't configure this policy setting computers use locally configured settings.

Printing.admx (Enable device control printing restrictions)

- Location: Machine
- Policy path: `Printers`
- Policy setting name: Enable Device Control Printing Restrictions
- Registry information: `HKLM\Software\Policies\Microsoft\Windows NT\Printers!EnableDeviceControl`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

Determines whether Device Control Printing Restrictions are enforced for printing on this computer.

By default there are no restrictions to printing based on connection type or printer Make/Model.

- If you turn on this setting, the computer restricts printing to printer connections on the corporate network or approved USB-connected printers.
- If you turn off this setting or don't configure it, there are no restrictions to printing based on connection type or printer Make/Model.

Printing.admx (Approved USB-connected print devices)

- Location: Machine
- Policy path: `Printers`
- Policy setting name: List of Approved USB-connected print devices
- Registry information: `HKLM\Software\Policies\Microsoft\Windows NT\Printers!ApprovedUsbPrintDevices`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

This setting is a component of the Device Control Printing Restrictions. To use this setting, turn on the **Enable Device Control Printing Restrictions** setting.

When Device Control Printing is turned on, the system uses the specified list of vid/pid values to determine if the current USB connected printer is approved for local printing. Enter all the approved vid/pid combinations (separated by commas) that correspond to approved USB printer models.

When a user tries to print to a USB printer queue, the device vid/pid is compared to the approved list.

StartMenu.admx

- Location: Machine
- Policy path: `Start Menu and Taskbar`
- Policy setting name: Show or hide "Most used" list from Start menu
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\Explorer!ShowOrHideMostUsedApps`
- Supported on: At least Windows Server 2016 Windows 10 Version 2106
- Setting value: -

If you turn on this policy setting, you can configure Start menu to show or hide the list of user's most used apps regardless of user settings.

- Select **Show** to force the Most used list to be shown and user can't change to hide it using the Settings app.

- Select **Hide** to force the "Most used" list to be hidden and user can't change to show it using the Settings app.
- Select **Not Configured**, turn off or don't configure this policy setting for users to turn on or off the display of Most used list using the Settings app. This is default behavior.

Configuring this policy to **Show** or **Hide** on supported versions of Windows 10 takes precedence over any setting used with the **Remove frequent programs list from the Start Menu** policy setting. The **Remove frequent programs list from the Start Menu** setting manages same part of Start menu but with fewer options.

WPN.admx

- Location: Machine
- Policy path: `Start Menu and Taskbar\Notifications`
- Policy setting name: Enables group policy for the WNS FQDN
- Registry information: `HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\PushNotifications!WnsEndpoint`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

This policy sets a special WNS FQDN for specific environments.

DeviceInstallation.admx

- Location: Machine
- Policy path: `System\Device Installation\Device Installation Restrictions`
- Policy setting name: Apply layered order of evaluation for Allow and Prevent device installation policies across all device match criteria
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\DeviceInstall\Restrictions!AllowDenyLayered`
- Supported on: At least Windows Server 2016 Windows 10 Version 2106
- Setting value: -

This policy setting changes the evaluation order in which Allow and Prevent policy settings are applied when more than one install policy setting is applicable for a given device.

Turn on this policy setting to ensure that overlapping device match criteria is applied based on an established hierarchy where more specific match criteria supersede less specific match criteria.

The hierarchical order of evaluation for policy settings that specify device match criteria is Device instance IDs > Device IDs > Device setup class > Removable devicesDevice instance IDs1. Prevent installation of devices using drivers that match these device instance IDs2.

- Allow installation of devices using drivers that match these device instance `IDsDevice IDs3`.
- Prevent installation of devices using drivers that match these device `IDs4`.
- Allow installation of devices using drivers that match these device `IDsDevice setup class5`.
- Prevent installation of devices using drivers that match these device setup `classes6`.
- Allow installation of devices using drivers that match these device setup `classesRemovable devices7`.
- Prevent installation of removable devices. This policy setting provides more granular control than the **Prevent installation of devices not described by other policy settings** policy setting.

If these conflicting policy settings are turned on at the same time, the **Apply layered order of evaluation for Allow and Prevent device installation policies across all device match criteria** policy setting is enabled and the other policy settings are ignored. If you turn off or don't configure this policy setting, the default evaluation is used.

By default, all **Prevent installation...** policy settings have precedence over any other policy setting that allows Windows to install a device.

FileSys.admx (Enable NTFS nonpaged pool usage)

- Location: Machine
- Policy path: `System\Filesystem\NTFS`
- Policy setting name: Enable NTFS nonpaged pool usage
- Registry information: `HKLM\System\CurrentControlSet\Policies!NtfsForceNonPagedPoolAllocation`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

By default, NTFS allocates memory from both pageable and nonpageable memory as needed. Turning on this setting tells NTFS to use nonpageable memory for all allocations. NTFS also changes all of its code sections to be nonpageable. The benefit of turning on this feature is a reduction in page-faults and stack usage at the cost of more memory consumption. A restart is required for this setting to take effect.

FileSys.admx (NTFS default tier)

- Location: Machine
- Policy path: `System\Filesystem\NTFS`
- Policy setting name: NTFS default tier
- Registry information: `HKLM\System\CurrentControlSet\Policies!NtfsDefaultTier`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

For NTFS tiered volumes, this setting controls the tier that new allocations go to by default. Client systems default to the Performance tier. Server systems default to the Capacity tier.

FileSys.admx (NTFS parallel flush threshold)

- Location: Machine
- Policy path: `System\Filesystem\NTFS`
- Policy path setting name: NTFS parallel flush threshold
- Registry information: `HKLM\System\CurrentControlSet\Policies!NtfsParallelFlushThreshold`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

When flushing modified file data from memory, NTFS chooses to use one or more threads based on how many files are currently open. This setting gives control over the open file threshold used to trigger parallel flush.

FileSys.admx (NFTS parallel flush worker threads)

- Location: Machine
- Policy path: `System\Filesystem\NTFS`

- Policy setting name: NTFS parallel flush worker threads
- Registry information: `HKLM\System\CurrentControlSet\Policies!NtfsParallelFlushWorkers`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

When flushing modified file data from memory, NTFS chooses to use one or more threads based on how many files are currently open. This setting gives control over how many threads are used. Making this value larger may decrease the time it takes to flush a volume, but the flush may have a larger impact on other concurrent IO operations. Values with special meaning:

- **0**: Use the system calculated default
- **1**: Disable parallel flush

The default value and limit for this setting varies based on the number of available processors on a given system. The default value calculation is: `(([NumProcessors]/2) + 1) - Default max value calculation is: ([NumProcessors]*2)`

Kerberos.admx

- Location: Machine
- Policy path: `System\Kerberos`
- Policy setting name: Allow retrieving the cloud kerberos ticket during the sign-in
- Registry information: `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters!CloudKerberosTicketRetrievalEnabled`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

This policy setting allows retrieving the cloud kerberos ticket during the sign-in.

- If you turn off or don't configure this policy setting, the cloud kerberos ticket isn't retrieved during the sign-in.
- If you turn on this policy setting, the cloud kerberos ticket is retrieved during the sign-in.

Netlogon.admx

- Location: Machine
- Policy path: `System\Net Logon\DC Locator DNS Records`
- Policy setting name: Use lowercase DNS host names when registering domain controller SRV records
- Registry information: `HKLM\Software\Policies\Microsoft\Netlogon\Parameters!DnsSrvRecordUseLowerCaseHostNames`
- Supported on: Unknown
- Setting value: -

This policy setting configures whether the domain controllers to which this setting is applied will lowercase their DNS host name when registering SRV records.

If you turn on this setting, the domain controllers will lowercase their DNS host name when registering domain controller SRV records. A best-effort attempt is made to delete any previously registered SRV records that contain mixed-case DNS host names. For more information and potential manual cleanup procedures, see Lowercase host names record.

- If you turn off this setting, the domain controllers use their configured DNS host name as-is when registering domain controller SRV records.
- If not configured, domain controllers default to using their local configuration. The default local configuration is enabled. A restart isn't required for changes to this setting to take effect.

sam.admx

- Location: Machine
- Policy path: `System\Security Account Manager`
- Policy setting name: Configure validation of ROCA-vulnerable WHfB keys during authentication
- Registry information: `HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\SAM!SamNGCKeyROCAValidation`
- Supported on: At least Windows Vista
- Setting value: -

This policy setting allows you to configure how domain controllers handle Windows Hello for Business (WHfB) keys that are vulnerable to the "Return of Coppersmith's attack" (ROCA) vulnerability. For more information, see ROCA vulnerability.

If you turn on this policy setting, the following options are supported:

- **Ignore**: during authentication, the domain controller doesn't probe any WHfB keys for the ROCA vulnerability
- **Audit**: during authentication, the domain controller emits audit events for WHfB keys that are subject to the ROCA vulnerability (authentications still succeeds).
- **Block**: during authentication, the domain controller blocks the use of WHfB keys that are subject to the ROCA vulnerability (authentications fails). This setting only takes effect on domain controllers.

If not configured, the domain controllers default to using their local configuration. The default local configuration is Audit. A reboot isn't required for changes to this setting to take effect.

To avoid unexpected disruptions, this setting shouldn't be set to Block until appropriate remediations have been performed for example patching of vulnerable TPMs

AppxPackageManager.admx (Archive infrequently used apps)

- Location: Machine
- Policy path: `Windows Components\App Package Deployment`
- Policy setting name: Archive infrequently used apps
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\Appx!AllowAutomaticAppArchiving`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

This policy setting controls whether the system can archive infrequently used apps.

- If you turn on this policy setting, the system periodically checks for and archives infrequently used apps.
- If you turn off this policy setting, then the system doesn't archive any apps.
- If you don't configure this policy setting (default), the system follows default behavior that is to periodically check for and archive infrequently used apps and the user can configure this setting themselves.

AppxPackageManager.admx (Don't allow sideloaded apps to automatically update)

- Location: Machine
- Policy path: `Windows Components\App Package Deployment`
- Policy setting name: Don't allow sideloaded apps to automatically update in the background
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\Appx!DisableBackgroundAutoUpdates`
- Supported on: At least Windows Server 2016 Windows 10 Version 2106
- Setting value: -

Manages a sideloaded apps' ability to automatically update in the background.

- If you turn on this policy, sideloaded apps don't automatically update in the background.
- If you turn off this policy, sideloaded apps automatically updates in the background. Default is 'disabled' (key not present).

AppxPackageManager.admx (Don't allow sideloaded apps to automatically update on metered network)

- Location: Machine
- Policy path: `Windows Components\App Package Deployment`
- Policy setting name: Don't allow sideloaded apps to automatically update in the background on a metered network
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\Appx!DisableMeteredNetworkBackgroundAutoUpdates`
- Supported on: At least Windows Server 2016 Windows 10 Version 2106
- Setting value: -

Manages a sideloaded apps' ability to automatically update in the background on a metered network.

- If you turn on this policy, sideloaded apps don't automatically update in the background on a metered network.
- If you turn off this policy, sideloaded apps automatically updates in the background on a metered network. Default is 'disabled' (key not present).

AppPrivacy.admx (Let Windows apps take screenshots)

- Location: Machine
- Policy path: `Windows Components\App Privacy`
- Policy setting name: Let Windows apps take screenshots of various windows or displays
- Registry information:
  - `HKLM\Software\Policies\Microsoft\Windows\AppPrivacy!LetAppsAccessGraphicsCaptureProgrammatic` <
  - `HKLM\Software\Policies\Microsoft\Windows\AppPrivacy!LetAppsAccessGraphicsCaptureProgrammatic_UserInControlOfTheseApps`
  - `HKLM\Software\Policies\Microsoft\Windows\AppPrivacy!LetAppsAccessGraphicsCaptureProgrammatic_ForceAllowTheseApps`
  - `HKLM\Software\Policies\Microsoft\Windows\AppPrivacy!LetAppsAccessGraphicsCaptureProgrammatic_ForceDenyTheseApps`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

This policy setting specifies whether Windows apps can take screenshots of various windows or displays. You can specify either a default setting for all apps or a per-app setting by specifying a Package Family Name. You can get the Package Family Name for an app by using the `Get-AppPackage Windows PowerShell cmdlet`. A per-app setting overrides the default setting.

- **User is in control** option: employees in your organization can decide whether Windows apps can take screenshots of various windows or displays by using Settings > Privacy on the device.
- **Force Allow** option: Windows apps are allowed to take screenshots of various windows or displays and employees in your organization can't change it.
- **Force Deny** option: Windows apps aren't allowed to take screenshots of various windows or displays and employees in your organization can't change it.

If you turn off or don't configure this policy setting, employees in your organization can decide whether Windows apps can take screenshots of various windows or displays by using Settings > Privacy on the device.

If an app is open when this Group Policy object is applied on a device, employees must restart the app or device for the policy changes to be applied to the app.

AppPrivacy.admx (Let Windows apps turn off screenshot border)

- Location: Machine
- Policy path: `Windows Components\App Privacy`
- Policy setting name: Let Windows apps turn off the screenshot border
  - `HKLM\Software\Policies\Microsoft\Windows\AppPrivacy!LetAppsAccessGraphicsCaptureWithoutBorder`
  - `HKLM\Software\Policies\Microsoft\Windows\AppPrivacy!LetAppsAccessGraphicsCaptureWithoutBorder_UserInControlOfTheseApps`
  - `HKLM\Software\Policies\Microsoft\Windows\AppPrivacy!LetAppsAccessGraphicsCaptureWithoutBorder_ForceAllowTheseApps`
  - `HKLM\Software\Policies\Microsoft\Windows\AppPrivacy!LetAppsAccessGraphicsCaptureWithoutBorder_ForceDenyTheseApps`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

This policy setting specifies whether Windows apps can turn off the screenshot border. You can specify either a default setting for all apps or a per-app setting by specifying a Package Family Name. You can get the Package Family Name for an app by using the Get-AppPackage Windows PowerShell cmdlet. A per-app setting overrides the default setting.

- **User is in control** option: employees in your organization can decide whether Windows apps can turn off the screenshot border by using Settings > Privacy on the device.
- **Force Allow** option: Windows apps are allowed to turn off the screenshot border and employees in your organization can't change it.
- **Force Deny** option: Windows apps aren't allowed to turn off the screenshot border and employees in your organization can't change it.

If you turn off or don't configure this policy setting, employees in your organization can decide whether Windows apps can turn off the screenshot border by using Settings > Privacy on the device.

If an app is open when this Group Policy object is applied on a device, employees must restart the app or device for the policy changes to be applied to the app.

Taskbar.admx

- Location: Machine
- Policy path: `Windows Components\Chat`
- Policy setting name: Configures the Chat icon on the taskbar
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\Windows Chat!ChatIcon`
- Supported on: At least Windows Server 2016 Windows 10
- Setting value: -

This policy setting allows you to configure the Chat icon on the taskbar.

- If you enable this policy setting and set it to **Show**, the Chat icon is displayed on the taskbar by default. Users can show or hide it in Settings.
- If you enable this policy setting and set it to **Hide**, the Chat icon is hidden by default. Users can show or hide it in Settings.
- If you turn on this policy setting and set it to **Disabled**, the Chat icon isn't displayed and users can't show or hide it in Settings.
- If you turn off or don't configure this policy setting, the Chat icon is configured according to the defaults for your Windows edition.

CloudContent.admx

- Location: Machine
- Policy path: `Windows Components\Cloud Content`
- Policy setting name: Turn off cloud consumer account state content
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\CloudContent!DisableConsumerAccountStateContent`
- Supported on: At least Windows Server 2016 Windows 10 Version 1909
- Setting value: -

This policy setting lets you turn off cloud consumer account state content in all Windows experiences.

- If you turn on this policy, Windows experiences that use the cloud consumer account state content client component, shows the default fallback content.
- If you turn off or don't configure this policy, Windows experiences are able to use cloud consumer account state content.

DataCollection.admx (Disable OneSettings Downloads)

- Location: Machine
- Policy path: `Windows Components\Data Collection and Preview Builds`
- Policy setting name: Disable OneSettings Downloads
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\DataCollection!DisableOneSettingsDownloads`
- Supported on: At least Windows Server 2016 Windows 10 Version 1909
- Setting value: -

This policy setting controls whether Windows attempts to connect with the OneSettings service.

- If you turn on this policy, Windows doesn't attempt to connect with the OneSettings Service.
- If you turn off or don't configure this policy setting, Windows periodically attempts to connect with the OneSettings service to download configuration settings.

DataCollection.admx (Enable OneSettings Auditing)

- Location: Machine
- Policy path: `Windows Components\Data Collection and Preview Builds`
- Policy setting name: Enable OneSettings Auditing
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\DataCollection!EnableOneSettingsAuditing`

- Supported on: At least Windows Server 2016 Windows 10 Version 1909
- Setting value: -

This policy setting controls whether Windows records attempts to connect with the OneSettings service to the EventLog.

- If you turn on this policy, Windows records attempts to connect with the OneSettings service to the `Microsoft\Windows\Privacy-Auditing\Operational EventLog` channel.
- If you turn off or don't configure this policy setting, Windows doesn't record attempts to connect with the OneSettings service to the EventLog.

DataCollection.admx (Limit Diagnostic Log Collection)

- Location: Machine
- Policy path: `Windows Components\Data Collection and Preview Builds`
- Policy setting name: Limit Diagnostic Log Collection
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\DataCollection!LimitDiagnosticLogCollection`
- Supported on: At least Windows Server 2016 Windows 10 Version 1909
- Setting value: -

This policy setting controls whether more diagnostic logs are collected when more information is needed to troubleshoot a problem on the device. Diagnostic logs are only sent when the device has been configured to send optional diagnostic data.

- If you turn on this policy setting, diagnostic logs aren't collected.
- If you turn off or don't configure this policy setting, we might collect diagnostic logs if the device has been configured to send optional diagnostic data.

DataCollection.admx (Limit Dump Collection)

- Location: Machine
- Policy path: `Windows Components\Data Collection and Preview Builds`
- Policy setting name: Limit Dump Collection
- Registry information: `HKLM\Software\Policies\Microsoft\Windows\DataCollection!LimitDumpCollection`

- Supported on: At least Windows Server 2016 Windows 10 Version 1909
- Setting value: -

This policy setting limits the type of dumps that can be collected when more information is needed to troubleshoot a problem. Dumps are only sent when the device has been configured to send optional diagnostic data.

- If you turn on this setting, Windows Error Reporting is limited to sending kernel mini dumps and user mode triage dumps.
- If you turn off or don't configure this policy setting, we might collect full or heap dumps if the user has opted to send optional diagnostic data.

Sensors.admx (Force Instant Lock)

- Location: Machine
- Policy path: `Windows Components\Human Presence`
- Policy setting name: Force Instant Lock
- Registry information:
  `HKLM\Software\Policies\Microsoft\HumanPresence!ForceInstantLock;`
  `HKLM\Software\Policies\Microsoft\HumanPresence!ForceInstantLock`
- Supported on: At least Windows 10
- Setting value: -

Determines whether Lock on Leave is forced on/off by the MDM policy. The user can't change this setting and the toggle in the user experience is greyed out.

Sensors.admx (Force Instant Wake)

- Location: Machine
- Policy path: `Windows Components\Human Presence`
- Policy setting name: Force Instant Wake
- Registry information:
  `HKLM\Software\Policies\Microsoft\HumanPresence!ForceInstantWake;`
  `HKLM\Software\Policies\Microsoft\HumanPresence!ForceInstantWake`
- Supported on: At least Windows 10
- Setting value: -

Determines whether Wake On Arrival is forced on/off by the MDM policy. The user can't change this setting and the toggle in the user experience is greyed out.

Sensors.admx (Lock Timeout)

- Location: Machine
- Policy path: `Windows Components\Human Presence`
- Policy setting name: Lock Timeout
- Registry information: `HKLM\Software\Policies\Microsoft\HumanPresence!ForceLockTimeout`
- Supported on: At least Windows 10
- Setting value: -

Determines the timeout for Lock on Leave forced by the MDM policy. The user can't change this setting and the toggle in the user experience is greyed out.

inetres.admx

- Location: Machine
- Policy path: `Windows Components\Internet Explorer`
- Policy setting name: Replace JScript by loading `JScript9Legacy` in place of JScript via MSHTML/WebOC.
- Registry information: `HKLM\Software\Policies\Microsoft\Internet Explorer\Main!JScriptReplacement`
- Supported on: At least Internet Explorer 11.0
- Setting value: -

This policy setting specifies whether JScript or JScript9Legacy is loaded for MSHTML/WebOC based invocations. If you turn on this policy setting, `JScript9Legacy` is loaded in situations where JScript is instantiated. If you turn off this policy or don't configure it, then JScript is used.

WindowsDefender.admx (Configure scheduled task times randomization window)

- Location: Machine

- Policy path: Windows Components\Microsoft Defender Antivirus
- Policy setting name: Configure scheduled task times randomization window
- Registry information:
  - `HKLM\Software\Policies\Microsoft\Windows Defender!SchedulerRandomizationTime`
  - `HKLM\Software\Policies\Microsoft\Windows Defender!SchedulerRandomizationTime`
- Supported on: At least Windows Server 2012 Windows 8 or Windows RT
- Setting value: -

This policy setting allows you to configure the scheduled scan start time and the scheduled security intelligence update start time window (in hours).

- If you turn off or don't configure this setting, scheduled tasks will begin at a random time, within an interval of four hours, after the specified start time.
- If you turn on this setting, you must pick a randomization window in hours. The possible randomization window interval is between 1 and 23 hours. |

WindowsDefender.admx (Define the directory path to copy support log files)

- Location: Machine
- Policy path: `Windows Components\Microsoft Defender Antivirus`
- Policy setting name: Define the directory path to copy support log files
- Registry information: `HKLM\Software\Policies\Microsoft\Windows Defender!SupportLogLocation`
- Supported version: At least Windows Server 2016 Windows 10 Version 1607
- Setting value: -

This policy setting allows you to configure the directory path where the support log files would be copied to. The value of this setting should be a valid directory path.

- If you turn on this setting, the support log files are copied to the specified support log location path.
- If you disable or don't configure this setting, the support logs files aren't copied to any location.

WindowsDefender.admx (Define device control policy groups)

- Location: Machine
- Policy path: `Windows Components\Microsoft Defender Antivirus\Device Control`
- Policy setting name: Define device control policy groups
- Registry information: `HKLM\Software\Policies\Microsoft\Windows Defender\Device Control\Policy Groups!PolicyGroups`
- Supported on: Unknown
- Setting value: -

Follow the device control policy groups xml schema to fill out the policy groups data.

WindowsDefender.admx (Define device control policy rules)

- Location: Machine
- Policy path: `Windows Components\Microsoft Defender Antivirus\Device Control`
- Policy setting name: Define device control policy rules
- Registry information: `HKLM\Software\Policies\Microsoft\Windows Defender\Device Control\Policy Rules!PolicyRules`
- Supported on: Unknown
- Setting value: -

Follow the device control policy groups xml schema to fill out the policy groups data.

WindowsDefender.admx (IP Address Exclusions)

- Location: Machine
- Policy path: `Windows Components\Microsoft Defender Antivirus\Exclusions`
- Policy setting name: IP Address Exclusions
- Registry information:
  - `HKLM\Software\Policies\Microsoft\Windows Defender\Exclusions!Exclusions_IpAddresses`
  - `HKLM\Software\Policies\Microsoft\Windows Defender\Exclusions\IpAddresses`
- Supported on: At least Windows Server 2016 Windows 10 Version 1709
- Setting value: -

Allows an administrator to explicitly disable network packet inspection made by `wdnisdrv` on a particular set of IP addresses.

WindowsDefender.admx (Controls whether Network Protection can be configured into block or test mode on Windows Server)

- Location: Machine
- Policy path: `Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Network Protection`
- Policy setting name: Controls whether Network Protection can be configured into block or test mode on Windows Server.
- Registry information: `HKLM\Software\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\Network Protection!AllowNetworkProtectionOnWinServer`
- Supported on: At least Windows Server 2016 Windows 10 Version 1709
- Setting value: `Disabled`

This configuration is dependent on the `EnableNetworkProtection` configuration. If this configuration is false, `EnableNetworkProtection` is ignored otherwise network protection starts on Windows Server depending on the value of `EnableNetworkProtection`.

- **Disabled (Default)**: **Not Configured** or **Disabled**, network protection can't be configured into block or test mode on Windows Server.
- **Enabled**: Administrators can control whether Network Protection can be configured into block or test mode on Windows Server.

WindowsDefender.admx (Controls datagram processing for network protection.)

- Location: Machine
- Policy path: `Windows Components\Microsoft Defender Antivirus\Network Inspection System`
- Policy setting name: Controls datagram processing for network protection.
- Registry information: `HKLM\Software\Policies\Microsoft\Windows Defender\NIS!DisableDatagramProcessing`
- Supported on: At least Windows Server 2016 Windows 10 Version 1709
- Setting value: `Disabled`

This configuration is dependent on the `EnableNetworkProtection` configuration. If this configuration is false, `EnableNetworkProtection` is ignored otherwise network protection starts on Windows Server depending on the value of `EnableNetworkProtection`.

- **Disabled (Default)**: If **Not Configured** or **Disabled**, network protection can't be configured into block or test mode on Windows Server.
- **Enabled**: Administrators can control whether Network Protection can be configured into block or test mode on Windows Server.

WindowsDefender.admx (Turn on script scanning)

- Location: Machine
- Policy path: `Windows Components\Microsoft Defender Antivirus\Real-time Protection`
- Policy setting name: Turn on script scanning
- Registry information: `HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection!DisableScriptScanning`
- Supported on: At least Windows Server 2012 Windows 8 or Windows RT
- Setting value: -

This policy setting allows you to configure script scanning.

- If you turn on or don't configure this setting, script scanning is enabled.
- If you turn off this setting, script scanning is disabled.

WindowsDefender.admx (Allows Microsoft Defender Antivirus to update and communicate over a metered connection)

- Location: Machine
- Policy path: `Windows Components\Microsoft Defender Antivirus\Security Intelligence Updates`
- Policy setting name: Allows Microsoft Defender Antivirus to update and communicate over a metered connection.
- Registry information: `HKLM\Software\Policies\Microsoft\Windows Defender\Signature Updates!MeteredConnectionUpdates`

- Supported on: At least Windows Server 2012 Windows 8 or Windows RT
- Setting value: `Disabled`

Setting options:

- **Disabled (Default)**: Updates and communications aren't allowed over metered connections.
- **Enabled**: Allow managed devices to update through metered connections. Data charges may apply.

TerminalServer.admx (Allow UI Automation redirection)

- Location: Machine
- Policy path: `Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection`
- Policy setting name: Allow UI Automation redirection
- Registry information: `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services!EnableUiaRedirection`
- Supported on: Unknown
- Setting value: -

This policy setting determines whether User Interface (UI) Automation client applications running on the local computer can access UI elements on the server.

UI Automation:

- Gives programs access to most UI elements. You can use assistive technology products like Magnifier and Narrator that need to interact with the UI in order to work properly.

- Allows automated test scripts to interact with the UI. Remote Desktop sessions don't currently support UI Automation redirection.

- If you turn on or don't configure this policy setting, any UI Automation clients on your local computer can interact with remote apps. For example, you can use your local computer's Narrator and Magnifier clients to interact with UI on a web page you opened in a remote session.

- If you turn off this policy setting, UI Automation clients running on your local computer can't interact with remote apps.

TerminalServer.admx (Don't allow location redirection)

- Location: Machine
- Policy path: `Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection`
- Policy setting name: Don't allow location redirection
- Registry information: `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services!fDisableLocationRedir`
- Supported on: Unknown
- Setting value: -

This policy setting lets you control the redirection of location data to the remote computer in a Remote Desktop Services session. By default, Remote Desktop Services allows redirection of location data.

- If you turn on this policy setting, users can't redirect their location data to the remote computer.
- If you turn off or don't configure this policy setting, users can redirect their location data to the remote computer. |

TenantRestrictions.admx

- Location: Machine
- Policy path: `Windows Components\Tenant Restrictions`
- Policy setting name: Cloud Policy Details
- Registry information:
  - `HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions\Payload!cloudid`
  - `HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions\Payload!tenantid`
  - `HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions\Payload!policyid`
  - `HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions\Payload!enforceFirewall`
  - `HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions\Payload!hostnames`

  - `HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions\Payload!subdomainSupportedHostnames`
  - `HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions\Payload!ipRanges`
- Supported on: At least Windows 10 Version 1909
- Setting value: -

This setting enables and configures the device-based tenant restrictions feature for Microsoft Entra ID. When you turn on this setting, compliant applications are prevented from accessing disallowed tenants according to a policy set in your Microsoft Entra tenant.

Creating a policy in your home tenant is required and more security measures for managed devices are recommended for best protection.

For more information, see Microsoft Entra tenant Restrictions before enabling firewall protection to ensure that a Windows Defender Application Control (WDAC) policy that correctly tags applications has been applied to the target devices.

Enabling firewall protection without a corresponding WDAC policy prevents all applications from reaching Microsoft endpoints. This firewall setting isn't supported on all versions of Windows. For more information, see setting up WDAC with tenant restrictions |

NewsAndInterests.admx

- Location: Machine
- Policy path: `Windows Components\Widgets`
- Policy setting name: Allow Widgets
- Registry information: `HKLM\SOFTWARE\Policies\Microsoft\Dsh!AllowNewsAndInterests`
- Supported on: At least Windows 10
- Setting value: -

This policy specifies whether the widgets feature is allowed on the device. Widgets are turned on by default unless you change this policy in your settings. If you turned on this setting before, it stays on automatically unless you turn it off.

Passport.admx

- Location: Machine
- Policy path: `Windows Components\Windows Hello for Business`
- Policy setting name: Use cloud trust for on-premises authentication

- Registry information: `HKLM\SOFTWARE\Policies\Microsoft\PassportForWork!UseCloudTrustForOnPremAuth`
- Supported on: At least Windows 10
- Setting value: -

Use this policy setting to configure Windows Hello for Business to use Microsoft Entra Kerberos for on-premises authentication.

- If you turn this policy setting, Windows Hello for Business uses a Kerberos ticket retrieved from authenticating to Azure for on-premises authentication.
- If you turn off or don't configure this policy setting, Windows Hello for Business uses a key or certificate (depending on other policy settings) for on-premises authentication.

An environment that enables both this policy setting and the **Use Windows Hello for Business** policy setting requires one or more Windows Server 2016 domain controllers. Otherwise, Windows Hello for Business authentication fails.

WindowsSandbox.admx (Allow audio input in Windows Sandbox)

- Location: Machine
- Policy path: `Windows Components\Windows Sandbox`
- Policy setting name: Allow audio input in Windows Sandbox
- Registry information: `HKLM\SOFTWARE\Policies\Microsoft\Windows\Sandbox!AllowAudioInput`
- Supported on: Unknown
- Setting value: -

This policy setting turns on or ogg audio input to the Sandbox.

- If you turn on this policy setting, Windows Sandbox can receive audio input from the user. Applications using a microphone may require this setting.
- If you turn off this policy setting, Windows Sandbox can't receive audio input from the user. Applications using a microphone may not function properly with this setting.
- If you don't configure this policy setting, audio input is enabled. There may be security implications of exposing host audio input to the container.

WindowsSandbox.admx (Allow clipboard sharing with Windows Sandbox)

- Location: Machine
- Policy path: `Windows Components\Windows Sandbox`
- Policy setting name: Allow clipboard sharing with Windows Sandbox
- Registry information: `HKLM\SOFTWARE\Policies\Microsoft\Windows\Sandbox!AllowClipboardRedirection`
- Supported on: Unknown
- Setting value: -

This policy setting enables or disables clipboard sharing with the sandbox.

- If you turn on this policy setting, copy and paste between the host, and Windows Sandbox are permitted.
- If you turn off this policy setting, copy and paste in and out of Sandbox is restricted.
- If you don't configure this policy setting, clipboard sharing is enabled.

WindowsSandbox.admx (Allow networking in Windows Sandbox)

- Location: Machine
- Policy path: `Windows Components\Windows Sandbox`
- Policy setting name: Allow networking in Windows Sandbox
- Registry information: `HKLM\SOFTWARE\Policies\Microsoft\Windows\Sandbox!AllowNetworking`
- Supported on: Unknown
- Setting value: `Disabled`

This policy setting turns on or off networking in the sandbox. You can disable network access to decrease the attack surface exposed by the sandbox.

- If you turn on this policy setting, networking is done by creating a virtual switch on the host and connects the Windows Sandbox to it via a virtual NIC. Turning on networking can expose untrusted applications to the internal network.
- If you turn off this policy setting, networking is disabled in Windows Sandbox. If you don't configure this policy setting, networking is enabled.

WindowsSandbox.admx (Allow printer sharing with Windows Sandbox)

- Location: Machine
- Policy path: `Windows Components\Windows Sandbox`
- Policy setting name: Allow printer sharing with Windows Sandbox
- Registry information: `HKLM\SOFTWARE\Policies\Microsoft\Windows\Sandbox!AllowPrinterRedirection`
- Supported on: Unknown
- Setting value: `Disabled`

This policy setting turns on or off printer sharing from the host into the Sandbox.

- If you turn on this policy setting, host printers are shared into Windows Sandbox.
- If you turn off this policy setting, Windows Sandbox can't view printers from the host.
- If you don't configure this policy setting, printer redirection is disabled.

WindowsSandbox.admx (Allow vGPU sharing for Windows Sandbox)

- Location: Machine
- Policy path: `Windows Components\Windows Sandbox`
- Policy setting name: Allow vGPU sharing for Windows Sandbox
- Registry information: `HKLM\SOFTWARE\Policies\Microsoft\Windows\Sandbox!AllowVGPU`
- Supported on: Unknown
- Setting value: `Disabled`

This policy setting turns on or off virtualized GPU.

- If you turn on this policy setting, vGPU is supported in the Windows Sandbox.
- If you turn off this policy setting, Windows Sandbox uses software rendering that can be slower than virtualized GPU.
- If you don't configure this policy setting, vGPU is turned on. Enabling virtualized GPU can potentially increase the attack surface of the sandbox.

WindowsSandbox.admx (Allow video input in Windows Sandbox)

- Location: Machine
- Policy path: `Windows Components\Windows Sandbox`
- Policy setting name: Allow video input in Windows Sandbox
- Registry information: `HKLM\SOFTWARE\Policies\Microsoft\Windows\Sandbox!AllowVideoInput`
- Supported on: Unknown
- Setting: `Disabled`

This policy setting turns on or off the video input to the Sandbox.

- If you turn on this policy setting, video input is enabled in Windows Sandbox.
- If you turn off this policy setting, video input is disabled in Windows Sandbox.
- If you don't configure this policy setting, video input is disabled. Applications that use video input might not function properly in Windows Sandbox. There may be security implications of exposing host video input to the container.

WindowsUpdate.admx

- Location: Machine
- Policy path: `Windows Components\Windows Update\Manage updates offered from Windows Server Update Service`
- Policy setting name: Specify source service for specific classes of Windows Updates
  - `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate\AU!UseUpdateClassPolicySource`
  - `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate!SetPolicyDrivenUpdateSourceForFeatureUpdates`
  - `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate!SetPolicyDrivenUpdateSourceForQualityUpdates`
  - `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate!SetPolicyDrivenUpdateSourceForDriverUpdates`
  - `HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate!SetPolicyDrivenUpdateSourceForOtherUpdates`
- Supported on: At least Windows Server 2016 Windows 10 Version 2106

- Setting value: -

When this policy is turned on, devices receive Windows updates for the classes listed from the specified update source: either Windows Update or Windows Server Update Service.

To receive any updates from the Windows Server Update Service, you must have properly configured an intranet Microsoft update service location via the **Specify intranet Microsoft update service location** policy.

- If this policy isn't configured or is turned off, the device continues to detect updates per your other policy configurations.
- If you're using the **Do not allow deferral policies to cause scans against Windows Update** policy to ensure devices only scan against your specified server, we recommend configuring this policy instead or in addition to that policy.