WindowsLogon Policy CSP

By officedocspr5

Archived: 2026-04-05 15:50:09 UTC

▶
▶

Tip

This CSP contains ADMX-backed policies which require a special SyncML format to enable or disable. You must specify the data type in the SyncML as `<Format>chr</Format>`. For details, see Understanding ADMX-backed policies.

The payload of the SyncML must be XML-encoded; for this XML encoding, there are a variety of online encoders that you can use. To avoid encoding the payload, you can use CDATA if your MDM supports it. For more information, see CDATA Sections.

AllowAutomaticRestartSignOn

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 10, version 1903 [10.0.18362] and later

```
./Device/Vendor/MSFT/Policy/Config/WindowsLogon/AllowAutomaticRestartSignOn
```

This policy setting controls whether a device will automatically sign in and lock the last interactive user after the system restarts or after a shutdown and cold boot.

This only occurs if the last interactive user didn't sign out before the restart or shutdown.

If the device is joined to Active Directory or Microsoft Entra ID, this policy only applies to Windows Update restarts. Otherwise, this will apply to both Windows Update restarts and user-initiated restarts and shutdowns.

- If you don't configure this policy setting, it's enabled by default. When the policy is enabled, the user is automatically signed in and the session is automatically locked with all lock screen apps configured for that user after the device boots.

After enabling this policy, you can configure its settings through the ConfigAutomaticRestartSignOn policy, which configures the mode of automatically signing in and locking the last interactive user after a restart or cold boot .

- If you disable this policy setting, the device doesn't configure automatic sign in. The user's lock screen apps aren't restarted after the system restarts.

Description framework properties:

Property name	Property value
Format	`chr` (string)
Access Type	Add, Delete, Get, Replace

Tip

This is an ADMX-backed policy and requires SyncML format for configuration. For an example of SyncML format, refer to Enabling a policy.

ADMX mapping:

Name	Value
Name	AutomaticRestartSignOn
Friendly Name	Sign-in and lock last interactive user automatically after a restart
Location	Computer Configuration
Path	Windows Components > Windows Logon Options
Registry Key Name	Software\Microsoft\Windows\CurrentVersion\Policies\System
Registry Value Name	DisableAutomaticRestartSignOn
ADMX File Name	WinLogon.admx

ConfigAutomaticRestartSignOn

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 10, version 1903 [10.0.18362] and later

```
./Device/Vendor/MSFT/Policy/Config/WindowsLogon/ConfigAutomaticRestartSignOn
```

This policy setting controls the configuration under which an automatic restart and sign-on and lock occurs after a restart or cold boot. If you chose "Disabled" in the "Sign-in and lock last interactive user automatically after a restart" policy, then automatic sign-on won't occur and this policy doesn't need to be configured.

- If you enable this policy setting, you can choose one of the following two options:

1. "Enabled if BitLocker is on and not suspended" specifies that automatic sign-on and lock will only occur if BitLocker is active and not suspended during the reboot or shutdown. Personal data can be accessed on the device's hard drive at this time if BitLocker isn't on or suspended during an update. BitLocker suspension temporarily removes protection for system components and data but may be needed in certain circumstances to successfully update boot-critical components.

BitLocker is suspended during updates if:

- The device doesn't have TPM 2.0 and PCR7, or
- The device doesn't use a TPM-only protector.

2. "Always Enabled" specifies that automatic sign-on will happen even if BitLocker is off or suspended during reboot or shutdown. When BitLocker isn't enabled, personal data is accessible on the hard drive. Automatic restart and sign-on should only be run under this condition if you are confident that the configured device is in a secure physical location.

- If you disable or don't configure this setting, automatic sign-on will default to the "Enabled if BitLocker is on and not suspended" behavior.

Description framework properties:

Property name	**Property value**
Format	`chr` (string)
Access Type	Add, Delete, Get, Replace

Tip

This is an ADMX-backed policy and requires SyncML format for configuration. For an example of SyncML format, refer to Enabling a policy.

ADMX mapping:

Name	**Value**
Name	ConfigAutomaticRestartSignOn

Name	Value
Friendly Name	Configure the mode of automatically signing in and locking last interactive user after a restart or cold boot
Location	Computer Configuration
Path	Windows Components > Windows Logon Options
Registry Key Name	Software\Microsoft\Windows\CurrentVersion\Policies\System
ADMX File Name	WinLogon.admx

DisableLockScreenAppNotifications

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 10, version 1703 [10.0.15063] and later

```
./Device/Vendor/MSFT/Policy/Config/WindowsLogon/DisableLockScreenAppNotifications
```

This policy setting allows you to prevent app notifications from appearing on the lock screen.

- If you enable this policy setting, no app notifications are displayed on the lock screen.
- If you disable or don't configure this policy setting, users can choose which apps display notifications on the lock screen.

Description framework properties:

Property name	Property value
Format	`chr` (string)
Access Type	Add, Delete, Get, Replace

Tip

This is an ADMX-backed policy and requires SyncML format for configuration. For an example of SyncML format, refer to Enabling a policy.

ADMX mapping:

Name	Value
Name	DisableLockScreenAppNotifications
Friendly Name	Turn off app notifications on the lock screen
Location	Computer Configuration
Path	System > Logon
Registry Key Name	Software\Policies\Microsoft\Windows\System
Registry Value Name	DisableLockScreenAppNotifications
ADMX File Name	Logon.admx

DontDisplayNetworkSelectionUI

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 10, version 1703 [10.0.15063] and later

```
./Device/Vendor/MSFT/Policy/Config/WindowsLogon/DontDisplayNetworkSelectionUI
```

This policy setting allows you to control whether anyone can interact with available networks UI on the logon screen.

- If you enable this policy setting, the PC's network connectivity state can't be changed without signing into Windows.
- If you disable or don't configure this policy setting, any user can disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.

Description framework properties:

Property name	Property value
Format	`chr` (string)
Access Type	Add, Delete, Get, Replace

Tip

This is an ADMX-backed policy and requires SyncML format for configuration. For an example of SyncML format, refer to Enabling a policy.

ADMX mapping:

Name	Value
Name	DontDisplayNetworkSelectionUI
Friendly Name	Do not display network selection UI
Location	Computer Configuration
Path	System > Logon
Registry Key Name	Software\Policies\Microsoft\Windows\System
Registry Value Name	DontDisplayNetworkSelectionUI
ADMX File Name	Logon.admx

Example:

Here's an example to enable this policy:

```
<SyncML xmlns="SYNCML:SYNCML1.2">
 <SyncBody>
   <Atomic>
     <CmdID>300</CmdID>
     <Replace>
       <CmdID>301</CmdID>
       <Item>
         <Target>
           <LocURI>./Device/Vendor/MSFT/Policy/Config/WindowsLogon/DontDisplayNetworkSelectionUI</LocURI>
         </Target>
         <Meta>
           <Format xmlns="syncml:metinf">chr</Format>
         </Meta>
         <Data><![CDATA[<enabled/>]]></Data>
       </Item>
     </Replace>
   </Atomic>
   <Final/>
  </SyncBody>
</SyncML>
```

EnableFirstLogonAnimation

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 10, version 1903 [10.0.18362] and later

```
./Device/Vendor/MSFT/Policy/Config/WindowsLogon/EnableFirstLogonAnimation
```

This policy setting allows you to control whether users see the first sign-in animation when signing in to the computer for the first time. This applies to both the first user of the computer who completes the initial setup and users who are added to the computer later. It also controls if Microsoft account users will be offered the opt-in prompt for services during their first sign-in.

- If you enable this policy setting, Microsoft account users will see the opt-in prompt for services, and users with other accounts will see the sign-in animation.
- If you disable this policy setting, users won't see the animation and Microsoft account users won't see the opt-in prompt for services.
- If you don't configure this policy setting, the user who completes the initial Windows setup will see the animation during their first sign-in. If the first user had already completed the initial setup and this policy setting isn't configured, users new to this computer won't see the animation.

Note

The first sign-in animation won't be shown on Server, so this policy will have no effect.

Description framework properties:

Property name	Property value
Format	`int`
Access Type	Add, Delete, Get, Replace
Default Value	1

Allowed values:

Value	Description
0	Disabled.

Value	Description
1 (Default)	Enabled.

Group policy mapping:

Name	Value
Name	EnableFirstLogonAnimation
Friendly Name	Show first sign-in animation
Location	Computer Configuration
Path	System > Logon
Registry Key Name	Software\Microsoft\Windows\CurrentVersion\Policies\System
Registry Value Name	EnableFirstLogonAnimation
ADMX File Name	Logon.admx

EnableMPRNotifications

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 11, version 22H2 [10.0.22621] and later

```
./Device/Vendor/MSFT/Policy/Config/WindowsLogon/EnableMPRNotifications
```

This policy controls whether the user's password is included in the content of MPR notifications sent by winlogon in the system.

- If you disable this setting or don't configure it, winlogon sends MPR notifications with empty password fields of the user's authentication info.
- If you enable this setting, winlogon sends MPR notifications containing the user's password in the authentication info.

Note

Starting in Windows Insiders build 25216, the behavior of EnableMPRNotifications policy was changed, and the Group Policy was updated with the following text:

- **Friendly name**: Configure the transmission of the user's password in the content of MPR notifications sent by winlogon
- **Description**: This policy controls whether the user's password is included in the content of MPR notifications sent by winlogon in the system.
    - If you disable this setting or do not configure it, winlogon sends MPR notifications with empty password fields of the user's authentication info.
    - If you enable this setting, winlogon sends MPR notifications containing the user's password in the authentication info.

Description framework properties:

Property name	Property value
Format	`chr` (string)
Access Type	Add, Delete, Get, Replace

Tip

This is an ADMX-backed policy and requires SyncML format for configuration. For an example of SyncML format, refer to Enabling a policy.

ADMX mapping:

Name	Value
Name	EnableMPRNotifications
Friendly Name	Configure the transmission of the user's password in the content of MPR notifications sent by winlogon.
Location	Computer Configuration
Path	Windows Components > Windows Logon Options
Registry Key Name	Software\Microsoft\Windows\CurrentVersion\Policies\System
Registry Value Name	EnableMPR
ADMX File Name	WinLogon.admx

EnumerateLocalUsersOnDomainJoinedComputers

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 10, version 1803 [10.0.17134] and later

```
./Device/Vendor/MSFT/Policy/Config/WindowsLogon/EnumerateLocalUsersOnDomainJoinedComputers
```

This policy setting allows local users to be enumerated on domain-joined computers.

- If you enable this policy setting, Logon UI will enumerate all local users on domain-joined computers.
- If you disable or don't configure this policy setting, the Logon UI won't enumerate local users on domain-joined computers.

Description framework properties:

Property name	Property value
Format	`chr` (string)
Access Type	Add, Delete, Get, Replace

Tip

This is an ADMX-backed policy and requires SyncML format for configuration. For an example of SyncML format, refer to Enabling a policy.

ADMX mapping:

Name	Value
Name	EnumerateLocalUsers
Friendly Name	Enumerate local users on domain-joined computers
Location	Computer Configuration
Path	System > Logon
Registry Key Name	Software\Policies\Microsoft\Windows\System
Registry Value Name	EnumerateLocalUsers
ADMX File Name	Logon.admx

HideFastUserSwitching

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 10, version 1703 [10.0.15063] and later

```
./Device/Vendor/MSFT/Policy/Config/WindowsLogon/HideFastUserSwitching
```

This policy setting allows you to hide the Switch User interface in the Logon UI, the Start menu and the Task Manager.

- If you enable this policy setting, the Switch User interface is hidden from the user who is attempting to log on or is logged-on to the computer that has this policy applied.

The locations that Switch User interface appear are in the Logon UI, the Start menu and the Task Manager.

- If you disable or don't configure this policy setting, the Switch User interface is accessible to the user in the three locations.

Description framework properties:

Property name	Property value
Format	`int`
Access Type	Add, Delete, Get, Replace
Default Value	0

Allowed values:

Value	Description
0 (Default)	Disabled (visible).
1	Enabled (hidden).

Group policy mapping:

Name	Value
Name	HideFastUserSwitching

Name	Value
Friendly Name	Hide entry points for Fast User Switching
Location	Computer Configuration
Path	System > Logon
Registry Key Name	Software\Microsoft\Windows\CurrentVersion\Policies\System
Registry Value Name	HideFastUserSwitching
ADMX File Name	Logon.admx

OverrideShellProgram

Scope	Editions	Applicable OS
✅ Device ❌ User	✅ Pro ✅ Enterprise ✅ Education ✅ IoT Enterprise / IoT Enterprise LTSC	✅ Windows 11, version 22H2 [10.0.22621.2338] and later

```
./Device/Vendor/MSFT/Policy/Config/WindowsLogon/OverrideShellProgram
```

OverrideShellProgram policy allows IT admin to configure the shell program for Windows OS on a device. This policy has the highest precedence over other ways of configuring the shell program. The policy currently supports below options: 1. Not Configured: Default shell will be launched. 2. Apply Lightweight Shell: Lightweight shell doesn't have a user interface and helps the device to achieve better performance as the shell consumes limited resources over default shell. Lightweight shell contains a limited set of features which could be consumed by applications. This configuration can be useful if the device needs to have a continuous running user interface application which would consume features offered by Lightweight shell. If you disable or don't configure this policy setting, then the default shell will be launched.

Description framework properties:

Property name	Property value
Format	`int`
Access Type	Add, Delete, Get, Replace
Default Value	0

Allowed values:

Value	Description
0 (Default)	Not Configured.
1	Apply Lightweight shell.

Related articles

Policy configuration service provider

Source: https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-windowslogon