Windows 10 (and later) settings to protect devices using Intune

- 03/13/2020
- To view the contributors to this article follow the link below

  (Follow this link https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-windows-10)

In this article

1. Before you begin
2. Microsoft Defender Application Guard
3. Microsoft Defender Firewall
4. Microsoft Defender SmartScreen settings
5. Windows Encryption
6. Microsoft Defender Exploit Guard
7. Microsoft Defender Application Control
8. Microsoft Defender Credential Guard
9. Microsoft Defender Security Center
10. Local device security options
11. Xbox services
12. Next steps

Microsoft Intune includes many settings to help protect your devices. This article describes all the settings you can enable and configure in Windows 10 and newer devices. These settings are created in an endpoint protection configuration profile in Intune to control security, including BitLocker and Microsoft Defender.

To configure Microsoft Defender Antivirus, see Windows 10 device restrictions.

Before you begin

Create an endpoint protection device configuration profile.

For more information about configuration service providers (CSPs), see Configuration service provider reference.

Microsoft Defender Application Guard

While using Microsoft Edge, Microsoft Defender Application Guard protects your environment from sites that aren't trusted by your organization. When users visit sites that aren't listed in your

isolated network boundary, the sites open in a Hyper-V virtual browsing session. Trusted sites are defined by a network boundary, which are configured in Device Configuration.

Application Guard is only available for Windows 10 (64-bit) devices. Using this profile installs a Win32 component to activate Application Guard.

- **Application Guard**
  Default: Not configured
  Application Guard CSP: Settings/AllowWindowsDefenderApplicationGuard
  - **Enabled for Edge** - Turns on this feature, which opens untrusted sites in a Hyper-V virtualized browsing container.
  - **Not configured** - Any site (trusted and untrusted) can open on the device.
- **Clipboard behavior**
  Default: Not configured
  Application Guard CSP: Settings/ClipboardSettings

  Choose what copy and paste actions are allowed between the local PC and the Application Guard virtual browser.

  - **Not configured**
  - **Allow copy and paste from PC to browser only**
  - **Allow copy and paste from browser to PC only**
  - **Allow copy and paste between PC and browser**
  - **Block copy and paste between PC and browser**

- **Clipboard content**
  This setting is available only when *Clipboard behavior* is set to one of the *allow* settings.
  Default: Not configured
  Application Guard CSP: Settings/ClipboardFileType

  Select the allowed clipboard content.

  - **Not configured**
  - **Text**
  - **Images**
  - **Text and images**
- **External content on enterprise sites**
  Default: Not configured
  Application Guard CSP: Settings/BlockNonEnterpriseContent
  - **Block** - Block content from unapproved websites from loading.
  - **Not configured** - Non-enterprise sites can open on the device.
- **Print from virtual browser**
  Default: Not configured
  Application Guard CSP: Settings/PrintingSettings
  - **Allow** - Allows the printing of selected content from the virtual browser.
  - **Not configured** Disable all print features.

When you *Allow* printing, you then can configure the following setting:

    - **Printing type(s)** Select one or more of the following options:
        - PDF
        - XPS
        - Local printers
        - Network printers

- **Collect logs**
  Default: Not configured
  Application Guard CSP: Audit/AuditApplicationGuard
    - **Allow** - Collect logs for events that occur within an Application Guard browsing session.
    - **Not configured** - Don't collect any logs within the browsing session.
- **Retain user-generated browser data**
  Default: Not configured
  Application Guard CSP: Settings/AllowPersistence
    - **Allow** Save user data (such as passwords, favorites, and cookies) that's created during an Application Guard virtual browsing session.
    - **Not configured** Discard user-downloaded files and data when the device restarts, or when a user signs out.
- **Graphics acceleration**
  Default: Not configured
  Application Guard CSP: Settings/AllowVirtualGPU
    - **Enable** - Load graphic-intensive websites and video faster by getting access to a virtual graphics processing unit.
    - **Not configured** Use the device's CPU for graphics; Don't use the virtual graphics processing unit.
- **Download files to host file system**
  Default: Not configured
  Application Guard CSP: Settings/SaveFilesToHost
    - **Enable** - Users can download files from the virtualized browser onto the host operating system.
    - **Not configured** - Keeps the files local on the device, and doesn't download files to the host file system.

Microsoft Defender Firewall

Global settings

These settings are applicable to all network types.

- **File Transfer Protocol**
  Default: Not configured
  Firewall CSP: MdmStore/Global/DisableStatefulFtp
    - **Block** - Disable stateful FTP.

    - **Not configured** - The firewall does stateful FTP filtering to allow secondary connections.
- **Security association idle time before deletion**
  Default: *Not configured*
  Firewall CSP: MdmStore/Global/SaIdleTime

  Specify an idle time in seconds, after which security associations are deleted.

- **Pre-shared key encoding**
  Default: Not configured
  Firewall CSP: MdmStore/Global/PresharedKeyEncoding
    - **Enable** - Encode presheared keys using UTF-8.
    - **Not configured** - Encode presheared keys using the local store value.
- **IPsec exemptions**
  Default: *0 selected*
  Firewall CSP: MdmStore/Global/IPsecExempt

  Select one or more of the following types of traffic to be exempt from IPsec:

    - **Neighbor discover IPv6 ICMP type-codes**
    - **ICMP**
    - **Router discover IPv6 ICMP type-codes**
    - **Both IPv4 and IPv6 DHCP network traffic**
- **Certificate revocation list verification**
  Default: Not configured
  Firewall CSP: MdmStore/Global/CRLcheck

  Choose how the device verifies the certificate revocation list. Options include:

    - **Disable CRL verification**
    - **Fail CRL verification on revoked certificate only**
    - **Fail CRL verification on any error encountered**.
- **Opportunistically match authentication set per keying module**
  Default: Not configured
  Firewall CSP: MdmStore/Global/OpportunisticallyMatchAuthSetPerKM
    - **Enable** Keying modules must ignore only the authentication suites that they don't support.
    - **Not configured**, Keying modules must ignore the entire authentication set if they don't support all of the authentication suites specified in the set.
- **Packet queuing**
  Default: Not configured
  Firewall CSP: MdmStore/Global/EnablePacketQueue

  Specify how software scaling on the receive side is enabled for the encrypted receive and clear text forward for the IPsec tunnel gateway scenario. This setting confirms the packet order is preserved. Options include:

- **Not configured**
- **Disable all packet queuing**
- **Queue inbound encrypted packets only**
- **Queue packets after decryption is performed for forwarding only**
- **Configure both inbound and outbound packets**

Network settings

The following settings are each listed in this article a single time, but all apply to the three specific network types:

- **Domain (workplace) network**
- **Private (discoverable) network**
- **Public (non-discoverable) network**

General settings

- **Microsoft Defender Firewall**
  Default: Not configured
  Firewall CSP: EnableFirewall
  - **Enable** - Turn on the firewall, and advanced security.
  - **Not configured** Allows all network traffic, regardless of any other policy settings.
- **Stealth mode**
  Default: Not configured
  Firewall CSP: DisableStealthMode
  - **Not configured**
  - **Block** - Firewall is blocked from operating in stealth mode. Blocking stealth mode allows you to also block **IPsec secured packet exemption**.
  - **Allow** - The firewall operates in stealth mode, which helps prevent responses to probing requests.
- **IPsec secured packet exemption with Stealth Mode**
  Default: Not configured
  Firewall CSP: DisableStealthModeIpsecSecuredPacketExemption

  This option is ignored if *Stealth mode* is set to *Block*.

  - **Not configured**
  - **Block** - IPSec secured packets do not receive exemptions.
  - **Allow** - Enable exemptions. The firewall's stealth mode MUST NOT prevent the host computer from responding to unsolicited network traffic that is secured by IPsec.
- **Shielded**
  Default: Not configured
  Firewall CSP: Shielded
  - **Not configured**
  - **Block** - When the Microsoft Defender Firewall is on and this setting is set to *Block*, all incoming traffic is blocked, regardless of other policy settings.

    - **Allow** - When set to *Allow*, this setting is turned off - and incoming traffic is allowed based on other policy settings.
- **Unicast responses to multicast broadcasts**
  Default: Not configured
  Firewall CSP: DisableUnicastResponsesToMulticastBroadcast

  Typically, you don't want to receive unicast responses to multicast or broadcast messages. These responses can indicate a denial of service (DOS) attack, or an attacker trying to probe a known live computer.

    - **Not configured**
    - **Block** - Disable unicast responses to multicast broadcasts.
    - **Allow** - Allow unicast responses to multicast broadcasts.
- **Inbound notifications**
  Default: Not configured
  Firewall CSP: DisableInboundNotifications
    - **Not configured**
    - **Block** - Hide notifications to uses when an app is blocked from listening on a port.
    - **Allow** - Enables this setting, and may show a notification to users when an app is blocked from listening on a port.
- **Default action for outbound connections**
  Default: Not configured
  Firewall CSP: DefaultOutboundAction

  Configure the default action firewall performs on outbound connections. This setting will get applied to Windows version 1809 and above.

    - **Not configured**
    - **Block** - The default firewall action isn't run on outbound traffic unless it's explicitly specified not to block.
    - **Allow** - Default firewall actions run on outbound connections.
- **Default action for inbound connections**
  Default: Not configured
  Firewall CSP: DefaultInboundAction
    - **Not configured**
    - **Block** - The default firewall action isn't run on inbound connections.
    - **Allow** - Default firewall actions run on inbound connections.

Rule merging

- **Authorized application Microsoft Defender Firewall rules from the local store**
  Default: Not configured
  Firewall CSP: AuthAppsAllowUserPrefMerge
    - **Not configured**
    - **Block** - The authorized application firewall rules in the local store are ignored and not enforced.

    - **Allow** - Choose **Enable** Applies firewall rules in the local store so they're recognized and enforced.
- **Global port Microsoft Defender Firewall rules from the local store**
  Default: Not configured
  Firewall CSP: GlobalPortsAllowUserPrefMerge
    - **Not configured**
    - **Block** - The global port firewall rules in the local store are ignored and not enforced.
    - **Allow** - Apply global port firewall rules in the local store to be recognized and enforced.
- **Microsoft Defender Firewall rules from the local store**
  Default: Not configured
  Firewall CSP: AllowLocalPolicyMerge
    - **Not configured**
    - **Block** - Firewall rules from the local store are ignored and not enforced.
    - **Allow** - Apply firewall rules in the local store to be recognized and enforced.
- **IPsec rules from the local store**
  Default: Not configured
  Firewall CSP: AllowLocalIpsecPolicyMerge
    - **Not configured**
    - **Block** - The connection security rules from the local store are ignored and not enforced, regardless of the schema version and connection security rule version.
    - **Allow** - Apply connection security rules from the local store, regardless of schema or connection security rule versions.

Firewall rules

You can **Add** one or more custom Firewall rules. For more information, see Add custom firewall rules for Windows 10 devices.

Custom Firewall rules support the following options:

General settings:

- **Name**
  Default: *No name*

  Specify a friendly name for your rule. This name will appear in the list of rules to help you identify it.

- **Description**
  Default: *No description*

  Provide a description of the rule.

- **Direction**
  Default: Not configured
  Firewall CSP: FirewallRules/*FirewallRuleName*/Direction

Specify if this rule applies to **Inbound**, or **Outbound** traffic. When set as **Not configured**, the rule automatically applies to Outbound traffic.

- **Action**
  Default: Not configured
  Firewall CSP: FirewallRules/*FirewallRuleName*/Action, and FirewallRules/*FirewallRuleName*/Action/Type

  Select from **Allow** or **Block**. When set as **Not configured**, the rule defaults to allow traffic.

- **Network type**
  Default: 0 selected
  Firewall CSP: FirewallRules/*FirewallRuleName*/Profiles

  Select up to three types of network types to which this rule belongs. Options include **Domain**, **Private**, and **Public**. If no network types are selected, the rule applies to all three network types.

Application settings

- **Application(s)**
  Default: All

  Control connections for an app or program. Select one of the following options, and then complete the additional configuration:

  - **Package family name** – Specify a package family name. To find the package family name, use the PowerShell command **Get-AppxPackage**.
    Firewall CSP: FirewallRules/*FirewallRuleName*/App/PackageFamilyName
  - **File path** – You must specify a file path to an app on the client device, which can be an absolute path, or a relative path. For example: C:\Windows\System\Notepad.exe or %WINDIR%\Notepad.exe.
    Firewall CSP: FirewallRules/*FirewallRuleName*/App/FilePath
  - **Windows service** – Specify the Windows service short name if it's a service and not an application that sends or receives traffic. To find the service short name, use the PowerShell command **Get-Service**.
    Firewall CSP: FirewallRules/*FirewallRuleName*/App/ServiceName
  - **All**– *No additional configuration is available*.

IP address settings

Specify the local and remote addresses to which this rule applies.

- **Local addresses**
  Default: Any address
  Firewall CSP: FirewallRules/*FirewallRuleName*/LocalPortRanges

  Select **Any address** or **Specified address**.

  When you use *Specified address*, you add one or more addresses as a comma-separated list of local addresses that are covered by the rule. Valid tokens include:

  - Use an asterisk "*" for *any* local address. If you use an asterisk, it must be the only token you use.
  - To specify a subnet use either the subnet mask or network prefix notation. If neither a subnet mask nor a network prefix is specified, the subnet mask defaults to 255.255.255.255.
  - A valid IPv6 address.
  - An IPv4 address range in the format of "start address - end address" with no spaces included.
  - An IPv6 address range in the format of "start address - end address" with no spaces included.
- **Remote addresses**
  Default: Any address
  Firewall CSP: FirewallRules/*FirewallRuleName*/RemoteAddressRanges

  Select **Any address** or **Specified address**.

  When you use *Specified address*, you add one or more addresses as a comma-separated list of remote addresses that are covered by the rule. Tokens aren't case-sensitive. Valid tokens include:

  - Use an asterisk "*" for *any* remote address. If you use an asterisk, it must be the only token you use.
  - "Defaultgateway"
  - "DHCP"
  - "DNS"
  - "WINS"
  - "Intranet" (supported on Windows versions 1809 and later)
  - "RmtIntranet" (supported on Windows versions 1809 and later)
  - "Internet" (supported on Windows versions 1809 and later)
  - "Ply2Renders" (supported on Windows versions 1809 and later)
  - "LocalSubnet" indicates any local address on the local subnet.
  - To specify a subnet use either the subnet mask or network prefix notation. If neither a subnet mask nor a network prefix is specified, the subnet mask defaults to 255.255.255.255.
  - A valid IPv6 address.
  - An IPv4 address range in the format of "start address - end address" with no spaces included.

- An IPv6 address range in the format of "start address - end address" with no spaces included.

Port and protocol settings

Specify the local and remote ports to which this rule applies.

- **Protocol**
  Default: Any
  Firewall CSP: FirewallRules/*FirewallRuleName*/Protocol
  Select from the following, and complete any required configurations:
  - **All –** No additional configuration is available.
  - **TCP –** Configure local and remote ports. Both options support All ports or Specified ports. Enter Specified ports by using a comma-separated list.
    - **Local ports** - Firewall CSP: FirewallRules/*FirewallRuleName*/LocalPortRanges
    - **Remote ports** - Firewall CSP: FirewallRules/*FirewallRuleName*/RemotePortRanges
  - **UDP –** Configure local and remote ports. Both options support All ports or Specified ports. Enter Specified ports by using a comma-separated list.
    - **Local ports** - Firewall CSP: FirewallRules/*FirewallRuleName*/LocalPortRanges
    - **Remote ports** - Firewall CSP: FirewallRules/*FirewallRuleName*/RemotePortRanges
  - **Custom –** Specify a custom **protocol** number from 0 to 255.

Advanced configuration

- **Interface types**
  Default: 0 selected
  Firewall CSP: FirewallRules/*FirewallRuleName*/InterfaceTypes

  Select from the following options:

  - **Remote access**
  - **Wireless**
  - **Local area network**
- **Only allow connections from these users**
  Default: All users *(Defaults to all uses when no list is specified)*
  Firewall CSP: FirewallRules/*FirewallRuleName*/LocalUserAuthorizationList

  Specify a list of authorized local users for this rule. A list of authorized users can't be specified if this rule applies to a Windows service.

Microsoft Defender SmartScreen settings

Microsoft Edge must be installed on the device.

- **SmartScreen for apps and files**
  Default: Not configured
  SmartScreen CSP: SmartScreen/EnableSmartScreenInShell
    - **Not configured** - Disables use of SmartScreen.
    - **Enable** - Enable Windows SmartScreen for file execution, and running apps. SmartScreen is a cloud-based anti-phishing and anti-malware component.
- **Unverified files execution**
  Default: Not configured
  SmartScreen CSP: SmartScreen/PreventOverrideForFilesInShell
    - **Not configured** - Disables this feature, and allows end users to run files that haven't been verified.
    - **Block** - Prevent end users from running files that haven't been verified by Windows SmartScreen.

Windows Encryption

Windows Settings

- **Encrypt devices**
  Default: Not configured
  BitLocker CSP: RequireDeviceEncryption
    - **Require** - Prompt users to enable device encryption. Depending on the Windows edition and system configuration, users may be asked:
        - To confirm that encryption from another provider isn't enabled.
        - Be required to turn off BitLocker Drive Encryption, and then turn BitLocker back on.
    - **Not configured**

  If Windows encryption is turned on while another encryption method is active, the device might become unstable.

- **Encrypt storage card (mobile only)**
  This setting only applies to Windows 10 mobile.
  Default: Not configured
  BitLocker CSP: RequireStorageCardEncryption
    - **Require** to encrypt any removable storage cards used by the device.
    - **Not configured** - Don't require storage card encryption, and don't prompt the user to turn it on.

BitLocker base settings

Base settings are universal BitLocker settings for all types of data drives. These settings manage what drive encryption tasks or configuration options the end user can modify across all types of data drives.

- **Warning for other disk encryption**
  Default: Not configured
  BitLocker CSP: AllowWarningForOtherDiskEncryption
    - **Block** - Disable the warning prompt if another disk encryption service is on the device.
    - **Not configured** - Allow the warning for other disk encryption to be shown.

  Tip

  To install BitLocker automatically and silently on a device that's Azure AD joined and runs Windows 1809 or later, this setting must be set to *Block*. For more information, see Silently enable BitLocker on devices.

  When set to *Block*, you can then configure the following setting:

    - **Allow standard users to enable encryption during Azure AD Join**
      This setting only applies to Azure Active Directory Joined (Azure ADJ) devices, and depends on the previous setting, `Warning for other disk encryption`.
      Default: Not configured
      BitLocker CSP: AllowStandardUserEncryption
        - **Allow** - Standard users (non-administrators) can enable BitLocker encryption when signed in.
        - **Not configured** only Administrators can enable BitLocker encryption on the device.

  Tip

- To install BitLocker automatically and silently on a device that's Azure AD joined and runs Windows 1809 or later, this setting must be set to *Allow*. For more information, see Silently enable BitLocker on devices.
- **Configure encryption methods**
  Default: Not configured
  BitLocker CSP: EncryptionMethodByDriveType
    - **Enable** - Configure encryption algorithms for operating system, data, and removable drives.
    - **Not configured** - BitLocker uses XTS-AES 128 bit as the default encryption method, or uses the encryption method specified by any setup script.

  When set to *Enable*, you can configure the following settings:

    - **Encryption for operating system drives**
      Default: XTS-AES 128-bit

      Choose the encryption method for operating system drives. We recommend you use the XTS-AES algorithm.

        - **AES-CBC 128-bit**
        - **AES-CBC 256-bit**

        - **XTS-AES 128-bit**
        - **XTS-AES 256-bit**
    - **Encryption for fixed data-drives**
      Default: AES-CBC 128-bit

      Choose the encryption method for fixed (built-in) data drives. We recommend you use the XTS-AES algorithm.

        - **AES-CBC 128-bit**
        - **AES-CBC 256-bit**
        - **XTS-AES 128-bit**
        - **XTS-AES 256-bit**
    - **Encryption for removable data-drives**
      Default: AES-CBC 128-bit

      Choose the encryption method for removable data drives. If the removable drive is used with devices that aren't running Windows 10, then we recommend you use the AES-CBC algorithm.

        - **AES-CBC 128-bit**
        - **AES-CBC 256-bit**
        - **XTS-AES 128-bit**
        - **XTS-AES 256-bit**

BitLocker OS drive settings

These settings apply specifically to operating system data drives.

- **Additional authentication at startup**
  Default: Not configured
  BitLocker CSP: SystemDrivesRequireStartupAuthentication
    - **Require** - Configure the authentication requirements for computer startup, including the use of Trusted Platform Module (TPM).
    - **Not configured** - Configure only basic options on devices with a TPM.

  When set to *Require*, you can configure the following settings:

    - **BitLocker with non-compatible TPM chip**
      Default: Not configured
        - **Block** - Disable use of BitLocker when a device doesn't have a compatible TPM chip.
        - **Not configured** - Users can use BitLocker without a compatible TPM chip. BitLocker may require a password or a startup key.
    - **Compatible TPM startup**
      Default: Allow TPM

      Configure if TPM is allowed, required, or not allowed.

- **Allow TPM**
- **Do not allow TPM**
- **Require TPM**

- **Compatible TPM startup PIN**
  Default: Allow startup PIN with TPM

  Choose to allow, not allow, or require using a startup PIN with the TPM chip. Enabling a startup PIN requires interaction from the end user.

  - **Allow startup PIN with TPM**
  - **Do not allow startup PIN with TPM**
  - **Require startup PIN with TPM**

  Tip

  To install BitLocker automatically and silently on a device that's Azure AD joined and runs Windows 1809 or later, this setting must not be set to *Require startup PIN with TPM*. For more information, see Silently enable BitLocker on devices.

- **Compatible TPM startup key**
  Default: Allow startup key with TPM

  Choose to allow, not allow, or require using a startup key with the TPM chip. Enabling a startup key requires interaction from the end user.

  - **Allow startup key with TPM**
  - **Do not allow startup key with TPM**
  - **Require startup key with TPM**

  Tip

  To install BitLocker automatically and silently on a device that's Azure AD joined and runs Windows 1809 or later, this setting must not be set to *Require startup key with TPM*. For more information, see Silently enable BitLocker on devices.

- **Compatible TPM startup key and PIN**
  Default: Allow startup key and PIN with TPM

  Choose to allow, not allow, or require using a startup key and PIN with the TPM chip. Enabling startup key and PIN requires interaction from the end user.

  - **Allow startup key and PIN with TPM**
  - **Do not allow startup key and PIN with TPM**
  - **Require startup key and PIN with TPM**

  Tip

To install BitLocker automatically and silently on a device that's Azure AD joined and runs Windows 1809 or later, this setting must not be set to *Require startup key and PIN with TPM*. For more information, see Silently enable BitLocker on devices.

- **Minimum PIN Length**
  Default: Not configured
  BitLocker CSP: SystemDrivesMinimumPINLength
  - **Enable** Configure a minimum length for the TPM startup PIN.
  - **Not configured** - Users can configure a startup PIN of any length between 6 and 20 digits.

  When set to *Enable*, you can configure the following setting:

  - **Minimum characters**
    Default: *Not configured* BitLocker CSP: SystemDrivesMinimumPINLength

    Enter the number of characters required for the startup PIN from **4-20**.

- **OS drive recovery**
  Default: Not configured
  BitLocker CSP: SystemDrivesRecoveryOptions
  - **Enable** - Control how BitLocker-protected operating system drives recover when the required start-up information isn't available.
  - **Not configured** - Default recovery options are supported for BitLocker recovery. By default, a DRA is allowed, the recovery options are chosen by the user, including the recovery password and recovery key, and recovery information isn't backed up to AD DS.

  When set to *Enable*, you can configure the following settings:

  - **Certificate-based data recovery agent**
    Default: Not configured
    - **Block** - Prevent use of data recovery agent with BitLocker-protected OS drives.
    - **Not configured** - Allow data recovery agents to be used with BitLocker-protected operating system drives.
  - **User creation of recovery password**
    Default: Allow 48-digit recovery password

    Choose if users are allowed, required, or not allowed to generate a 48-digit recovery password.

    - **Allow 48-digit recovery password**
    - **Do not allow 48-digit recovery password**
    - **Require 48-digit recovery password**
  - **User creation of recovery key**
    Default: Allow 256-bit recovery key

Choose if users are allowed, required, or not allowed to generate a 256-bit recovery key.

- **Allow 256-bit recovery key**
- **Do not allow 256-bit recovery key**
- **Require 256-bit recovery key**

- **Recovery options in the BitLocker setup wizard**
  Default: Not configured
  - **Block** - Users can't see and change the recovery options. When set to
  - **Not configured** - Users can see and change the recovery options when they turn on BitLocker.
- **Save BitLocker recovery information to Azure Active Directory**
  Default: Not configured
  - **Enable** - Store the BitLocker recovery information to Azure Active Directory (Azure AD).
  - **Not configured** - BitLocker recovery information isn't stored in AAD.
- **BitLocker recovery Information stored to Azure Active Directory**
  Default: Backup recovery passwords and key packages

  Configure what parts of BitLocker recovery information are stored in Azure AD. Choose from:

  - **Backup recovery passwords and key packages**
  - **Backup recovery passwords only**
- **Client-driven recovery password rotation**
  Default: Key rotation enabled for Azure AD-joined devices
  BitLocker CSP: ConfigureRecoveryPasswordRotation

  This setting initiates a client-driven recovery password rotation after an OS drive recovery (either by using bootmgr or WinRE).

  - Not configured
  - Key rotation disabled
  - Key rotation enabled for Azure AD-joined deices
  - Key rotation enabled for Azure AD and Hybrid-joined devices
- **Store recovery information in Azure Active Directory before enabling BitLocker**
  Default: Not configured

  Prevent users from enabling BitLocker unless the computer successfully backs up the BitLocker recovery information to Azure Active Directory.

  - **Require** - Stop users from turning on BitLocker unless the BitLocker recovery information is successfully stored in Azure AD.
  - **Not configured** - Users can turn on BitLocker, even if recovery information isn't successfully stored in Azure AD.

- **Pre-boot recovery message and URL**
  Default: Not configured
  BitLocker CSP: SystemDrivesRecoveryMessage
    - **Enable** - Configure the message and URL that display on the pre-boot key recovery screen.
    - **Not configured** - Disable this feature.

  When set to *Enable*, you can configure the following setting:

    - **Pre-boot recovery message**
      Default: Use default recovery message and URL

      Configure how the pre-boot recovery message displays to users. Choose from:

        - **Use default recovery message and URL**
        - **Use empty recovery message and URL**
        - **Use custom recovery message**
        - **Use custom recovery URL**

BitLocker fixed data-drive settings

These settings apply specifically to fixed data drives.

- **Write access to fixed data-drive not protected by BitLocker**
  Default: Not configured
  BitLocker CSP: FixedDrivesRequireEncryption
    - **Block** - Give read-only access to data drives that aren't BitLocker-protected.
    - **Not configured** - By default, read and write access to data drives that aren't encrypted.
- **Fixed drive recovery**
  Default: Not configured
  BitLocker CSP: FixedDrivesRecoveryOptions
    - **Enable** - Control how BitLocker-protected fixed drives recover when the required start-up information isn't available.
    - **Not configured** - Disable this feature.

  When set to *Enable*, you can configure the following settings:

    - **Data recovery agent**
      Default: Not configured
        - **Block** - Prevent use of the data recovery agent with BitLocker-protected fixed drives Policy Editor.
        - **Not configured** - Enables use of data recovery agents with BitLocker-protected fixed drives.
    - **User creation of recovery password**
      Default: Allow 48-digit recovery password

Choose if users are allowed, required, or not allowed to generate a 48-digit recovery password.

- **Allow 48-digit recovery password**
- **Do not allow 48-digit recovery password**
- **Require 48-digit recovery password**

- **User creation of recovery key**
  Default: Allow 256-bit recovery key

  Choose if users are allowed, required, or not allowed to generate a 256-bit recovery key.

  - **Allow 256-bit recovery key**
  - **Do not allow 256-bit recovery key**
  - **Require 256-bit recovery key**
- **Recovery options in the BitLocker setup wizard**
  Default: Not configured
  - **Block** - Users can't see and change the recovery options. When set to
  - **Not configured** - Users can see and change the recovery options when they turn on BitLocker.
- **Save BitLocker recovery information to Azure Active Directory**
  Default: Not configured
  - **Enable** - Store the BitLocker recovery information to Azure Active Directory (Azure AD).
  - **Not configured** - BitLocker recovery information isn't stored in AAD.
- **BitLocker recovery Information stored to Azure Active Directory**
  Default: Backup recovery passwords and key packages

  Configure what parts of BitLocker recovery information are stored in Azure AD. Choose from:

  - **Backup recovery passwords and key packages**
  - **Backup recovery passwords only**
- **Client-driven recovery password rotation**
  Default: Key rotation enabled for Azure AD-joined devices
  BitLocker CSP: ConfigureRecoveryPasswordRotation

  This setting initiates a client-driven recovery password rotation after an OS drive recovery (either by using bootmgr or WinRE).

  - Not configured
  - Key rotation disabled
  - Key rotation enabled for Azure AD-joined deices
  - Key rotation enabled for Azure AD and Hybrid-joined devices
- **Store recovery information in Azure Active Directory before enabling BitLocker**
  Default: Not configured

Prevent users from enabling BitLocker unless the computer successfully backs up the BitLocker recovery information to Azure Active Directory.

- **Require** - Stop users from turning on BitLocker unless the BitLocker recovery information is successfully stored in Azure AD.
- **Not configured** - Users can turn on BitLocker, even if recovery information isn't successfully stored in Azure AD.

BitLocker removable data-drive settings

These settings apply specifically to removable data drives.

- **Write access to removable data-drive not protected by BitLocker**
  Default: Not configured
  BitLocker CSP: RemovableDrivesRequireEncryption
  - **Block** - Give read-only access to data drives that aren't BitLocker-protected.
  - **Not configured** - By default, read and write access to data drives that aren't encrypted.

  When set to *Enable*, you can configure the following setting:

  - **Write access to devices configured in another organization**
    Default: Not configured
    - **Block** - Block write access to devices configured in another organization.
    - **Not configured** - Deny write access.

Microsoft Defender Exploit Guard

Use exploit protection to manage and reduce the attack surface of apps used by your employees.

Attack Surface Reduction

Attack surface reduction rules help prevent behaviors malware often uses to infect computers with malicious code.

Attack Surface Reduction rules

- **Flag credential stealing from the Windows local security authority subsystem**
  Default: Not configured
  Rule: Block credential stealing from the Windows local security authority subsystem (lsass.exe)

  Help prevent actions and apps that are typically used by exploit-seeking malware to infect machines.

  - **Not configured**

    - **Enable** - Flag credential stealing from the Windows local security authority subsystem (lsass.exe).
    - **Audit only**
- **Process creation from Adobe Reader (beta)**
  Default: Not configured
  Rule: Block Adobe Reader from creating child processes
    - **Not configured**
    - **Enable** - Block child processes that are created from Adobe Reader.
    - **Audit only**

Rules to prevent Office Macro threats

Block Office apps from taking the following actions:

- **Office apps injecting into other processes (no exceptions)**
  Default: Not configured
  Rule: Block Office applications from injecting code into other processes
    - **Not configured**
    - **Block** - Block Office apps from injecting into other processes.
    - **Audit only**
- **Office apps/macros creating executable content**
  Default: Not configured
  Rule: Block Office applications from creating executable content
    - **Not configured**
    - **Block** - Block Office apps and macros from creating executable content.
    - **Audit only**
- **Office apps launching child processes**
  Default: Not configured
  Rule: Block all Office applications from creating child processes
    - **Not configured**
    - **Block** - Block Office apps from launching child processes.
    - **Audit only**
- **Win32 imports from Office macro code**
  Default: Not configured
  Rule: Block Win32 API calls from Office macros
    - **Not configured**
    - **Block** - Block Win32 imports from macro code in Office.
    - **Audit only**
- **Process creation from Office communication products**
  Default: Not configured
  Rule: Block Office communication application from creating child processes
    - **Not configured**
    - **Enable** - Block child process creation from Office communications apps.
    - **Audit only**

Rules to prevent script threats

Block the following to help prevent against script threats:

- **Obfuscated js/vbs/ps/macro code**
  Default: Not configured
  Rule: Block execution of potentially obfuscated scripts
    - **Not configured**
    - **Block** - Block any obfuscated js/vbs/ps/macro code.
    - **Audit only**
- **js/vbs executing payload downloaded from Internet (no exceptions)**
  Default: Not configured
  Rule: Block JavaScript or VBScript from launching downloaded executable content
    - **Not configured**
    - **Block** - Block js/vbs from executing payload downloaded from Internet.
    - **Audit only**
- **Process creation from PSExec and WMI commands**
  Default: Not configured
  Rule: Block process creations originating from PSExec and WMI commands
    - **Not configured**
    - **Block** - Block process creations originating from PSExec and WMI commands.
    - **Audit only**
- **Untrusted and unsigned processes that run from USB**
  Default: Not configured
  Rule: Block untrusted and unsigned processes that run from USB
    - **Not configured**
    - **Block** - Block untrusted and unsigned processes that run from USB.
    - **Audit only**
- **Executables that don't meet a prevalence, age, or trusted list criteria**
  Default: Not configured
  Rule: Block executable files from running unless they meet a prevalence, age, or trusted list criterion
    - **Not configured**
    - **Block** - Block executable files from running unless they meet a prevalence, age, or trusted list criteria.
    - **Audit only**

Rules to prevent email threats

Block the following to help prevent email threats:

- **Execution of executable content (exe, dll, ps, js, vbs, etc.) dropped from email (webmail/mail client) (no exceptions)**
  Default: Not configured
  Rule: Block executable content from email client and webmail
    - **Not configured**

- **Block** - Block execution of executable content (exe, dll, ps, js, vbs, etc.) dropped from email (webmail/mail-client).
- **Audit only**

Rules to protect against ransomware

- **Advanced ransomware protection**
  Default: Not configured
  Rule: Use advanced protection against ransomware
  - **Not configured**
  - **Enable** - Use aggressive ransomware protection.
  - **Audit only**

Attack Surface Reduction exceptions

- **Files and folder to exclude from attack surface reduction rules**
  Defender CSP: AttackSurfaceReductionOnlyExclusions
  - **Import** a .csv file that contains files and folders to exclude from attack surface reduction rules.
  - **Add** local files or folders manually.

Important

To allow proper installation and execution of LOB Win32 apps, anti-malware settings should exclude the following directories from being scanned:
On X64 client machines:
C:\Program Files (x86)\Microsoft Intune Management Extension\Content
C:\windows\IMECache

On X86 client machines:
C:\Program Files\Microsoft Intune Management Extension\Content
C:\windows\IMECache

Controlled folder access

Help protect valuable data from malicious apps and threats, such as ransomware.

Folder protection

Default: Not configured

Defender CSP: EnableControlledFolderAccess

Protect files and folders from unauthorized changes by unfriendly apps.

Not configured

Enable

Audit only

Block disk modification

Audit disk modification

When you select a configuration other than Not configured, you can then configure:

List of apps that have access to protected folders

Defender CSP: ControlledFolderAccessAllowedApplications

Import a .csv file that contains an app list.

Add apps to this list manually.

List of additional folders that need to be protected

Defender CSP: ControlledFolderAccessProtectedFolders

Import a .csv file that contains a folder list.

Add folders to this list manually.

Network filtering

Block outbound connections from any app to IP addresses or domains with low reputations. Network filtering is supported in both Audit and Block mode.

Network protection

Default: Not configured

Defender CSP: EnableNetworkProtection

The intent of this setting is to protect end users from apps with access to phishing scams, exploit-hosting sites, and malicious content on the Internet. It also prevents third-party browsers from connecting to dangerous sites.

Not configured - Disable this feature. Users and apps aren't blocked from connecting to dangerous domains. Administrators can't see this activity in Microsoft Defender Security Center.

Enable - Turn on network protection, and block users and apps from connecting to dangerous domains. Administrators can see this activity in Microsoft Defender Security Center.

Audit only: - Users and apps aren't blocked from connecting to dangerous domains. Administrators can see this activity in Microsoft Defender Security Center.

Exploit protection

Upload XML

Default: Not configured

To use exploit protection to protect devices from exploits, create an XML file that includes the system and application mitigation settings you want. There are two methods to create the XML file:

PowerShell - Use one or more of the Get-ProcessMitigation, Set-ProcessMitigation, and ConvertTo-ProcessMitigationPolicy PowerShell cmdlets. The cmdlets configure mitigation settings, and export an XML representation of them.

Microsoft Defender Security Center UI - In the Microsoft Defender Security Center, click on App & browser control and then scroll to the bottom of the resulting screen to find Exploit Protection. First, use the System settings and Program settings tabs to configure mitigation settings. Then, find the Export settings link at the bottom of the screen to export an XML representation of them.

User editing of the exploit protection interface

Default: Not configured

ExploitGuard CSP: ExploitProtectionSettings

Block - Upload an XML file that allows you to configure memory, control flow, and policy restrictions. The settings in the XML file can be used to block an application from exploits.

Not configured - No custom configuration is used.

Microsoft Defender Application Control

Choose additional apps that either need to be audited by, or can be trusted to run by Microsoft Defender Application Control. Windows components and all apps from Windows store are automatically trusted to run.

Application control code integrity policies

Default: Not configured

CSP: AppLocker CSP

Enforce - Choose the application control code integrity policies for your users' devices.

After being enabled on a device, Application Control can only be disabled by changing the mode from Enforce to Audit only. Changing the mode from Enforce to Not Configured results in Application Control continuing to be enforced on assigned devices.

Not Configured - Application Control is not added to devices. However, settings that were previously added continue to be enforced on assigned devices.

Audit only - Applications aren't blocked. All events are logged in the local client's logs.

Microsoft Defender Credential Guard

Microsoft Defender Credential Guard protects against credential theft attacks. It isolates secrets so that only privileged system software can access them.

Credential Guard

Default: Disable

DeviceGuard CSP

Disable - Turn off Credential Guard remotely, if it was previously turned on with the Enabled without UEFI lock option.

Enable with UEFI lock - Credential Guard can't be disabled remotely by using a registry key or group policy.

Note

If you use this setting, and then later want to disable Credential Guard, you must set the Group Policy to Disabled. And, physically clear the UEFI configuration information from each computer. As long as the UEFI configuration persists, Credential Guard is enabled.

Enable without UEFI lock - Allows Credential Guard to be disabled remotely by using Group Policy. The devices that use this setting must be running Windows 10 version 1511 and newer.

When you enable Credential Guard, the following required features are also enabled:

Virtualization-based Security (VBS)

Turns on during the next reboot. Virtualization-based security uses the Windows Hypervisor to provide support for security services.

Secure Boot with Directory Memory Access

Turns on VBS with Secure Boot and direct memory access (DMA) protections. DMA protections require hardware support, and are only enabled on correctly configured devices.

Microsoft Defender Security Center

Microsoft Defender Security Center operates as a separate app or process from each of the individual features. It displays notifications through the Action Center. It acts as a collector or single place to see the status and run some configuration for each of the features. Find out more in the Microsoft Defender docs.

Microsoft Defender Security Center app and notifications

Block end-user access to the various areas of the Microsoft Defender Security Center app. Hiding a section also blocks related notifications.

Virus and threat protection

Default: Not configured

WindowsDefenderSecurityCenter CSP: DisableVirusUI

Configure if end users can view the Virus and threat protection area in the Microsoft Defender Security Center. Hiding this section will also block all notifications related to Virus and threat protection.

Not configured

Hide

Ransomware protection

Default: Not configured

WindowsDefenderSecurityCenter CSP: HideRansomwareDataRecovery

Configure if end users can view the Ransomware protection area in the Microsoft Defender Security Center. Hiding this section will also block all notifications related to Ransomware protection.

Not configured

Hide

Account protection

Default: Not configured

WindowsDefenderSecurityCenter CSP: DisableAccountProtectionUI

Configure if end users can view the Account protection area in the Microsoft Defender Security Center. Hiding this section will also block all notifications related to Account protection.

Not configured

Hide

Firewall and network protection

Default: Not configured

WindowsDefenderSecurityCenter CSP: DisableNetworkUI

Configure if end users can view the Firewall and network protection area in the Microsoft Defender Security center. Hiding this section will also block all notifications related to Firewall and network protection.

Not configured

Hide

App and browser Control

Default: Not configured

WindowsDefenderSecurityCenter CSP: DisableAppBrowserUI

Configure if end users can view the App and browser control area in the Microsoft Defender Security center. Hiding this section will also block all notifications related to App and browser control.

Not configured

Hide

Hardware protection

Default: Not configured

WindowsDefenderSecurityCenter CSP: DisableDeviceSecurityUI

Configure if end users can view the Hardware protection area in the Microsoft Defender Security Center. Hiding this section will also block all notifications related to Hardware protection.

Not configured

Hide

Device performance and health

Default: Not configured

WindowsDefenderSecurityCenter CSP: DisableHealthUI

Configure if end users can view the Device performance and health area in the Microsoft Defender Security center. Hiding this section will also block all notifications related to Device performance and health.

Not configured

Hide

Family options

Default: Not configured

WindowsDefenderSecurityCenter CSP: DisableFamilyUI

Configure if end users can view the Family options area in the Microsoft Defender Security center. Hiding this section will also block all notifications-related to Family options.

Not configured

Hide

Notifications from the displayed areas of app

Default: Not configured

WindowsDefenderSecurityCenter CSP: DisableNotifications

Choose which notifications to display to end users. Non-critical notifications include summaries of Microsoft Defender Antivirus activity, including notifications when scans have completed. All other notifications are considered critical.

Not configured

Block non-critical notifications

Block all notifications

Windows Security Center icon in the system tray

Default: Not configured

Configure the display of the notification area control. The user needs to either sign out and sign in or reboot the computer for this setting to take effect.

Not configured

Hide

Clear TPM button

Default: Not configured

Configure the display of the Clear TPM button.

Not configured

Disable

TPM firmware update warning

Default: Not configured

Configure the display of update TPM Firmware when a vulnerable firmware is detected.

Not configured

Hide

Tamper Protection

Default: Not configured

Turn Tamper Protection on or off on devices. To use Tamper Protection, you must integrate Microsoft Defender Advanced Threat Protection with Intune, and have Enterprise Mobility + Security E5 Licenses.

Not configured - No change is made to device settings.

Enabled - Tamper Protection is turned on and restrictions are enforced on devices.

Disabled - Tamper Protection is turned off and restrictions are not enforced.

IT contact Information

Provide IT contact information to appear in the Microsoft Defender Security Center app and the app notifications.

You can choose to Display in app and in notifications, Display only in app, Display only in notifications, or Don't display. Enter the IT organization name, and at least one of the following contact options:

IT contact information

Default: Don't display

WindowsDefenderSecurityCenter CSP: EnableCustomizedToasts

Configure where to display IT contact information to end users.

Display in app and in notifications

Display only in app

Display only in notifications

Don't display

When configured to display, you can configure the following settings:

IT organization name

Default: Not configured

WindowsDefenderSecurityCenter CSP: CompanyName

IT department phone number or Skype ID

Default: Not configured

WindowsDefenderSecurityCenter CSP: Phone

IT department email address

Default: Not configured

WindowsDefenderSecurityCenter CSP: Email

IT support website URL

Default: Not configured

WindowsDefenderSecurityCenter CSP: URL

Local device security options

Use these options to configure the local security settings on Windows 10 devices.

Accounts

Add new Microsoft accounts

Default: Not configured

LocalPoliciesSecurityOptions CSP: Accounts_BlockMicrosoftAccounts

Block Prevent users from adding new Microsoft accounts to the device.

Not configured - Users can use Microsoft accounts on the device.

Remote log on without password

Default: Not configured

LocalPoliciesSecurityOptions CSP: Accounts_LimitLocalAccountUseOfBlankPasswordsToConsoleLogonOnly

Block - Allow only local accounts with blank passwords to sign in using the device's keyboard.

Not configured - Allow local accounts with blank passwords to sign in from locations other than the physical device.

Admin

Local admin account

Default: Not configured

LocalPoliciesSecurityOptions CSP: Accounts_LimitLocalAccountUseOfBlankPasswordsToConsoleLogonOnly

Block Prevent use of a local admin account.

Not configured

Rename admin account

Default: Not configured

LocalPoliciesSecurityOptions CSP: Accounts_RenameAdministratorAccount

Define a different account name to be associated with the security identifier (SID) for the account "Administrator".

Guest

Guest account

Default: Not configured

LocalPoliciesSecurityOptions CSP: LocalPoliciesSecurityOptions

Block - Prevent use of a Guest account.

Not configured

Rename guest account

Default: Not configured

LocalPoliciesSecurityOptions CSP: Accounts_RenameGuestAccount

Define a different account name to be associated with the security identifier (SID) for the account "Guest".

Devices

Undock device without logon

Default: Not configured

LocalPoliciesSecurityOptions CSP: Devices_AllowUndockWithoutHavingToLogon

Block - Users can press a docked portable device's physical eject button to safely undock the device.

Not configured - A user must sign in to the device, and receive permission to undock the device.

Install printer drivers for shared printers

Default: Not configured

LocalPoliciesSecurityOptions CSP: Devices_PreventUsersFromInstallingPrinterDriversWhenConnectingToSharedPrinters

Enabled - Any user can install a printer driver as part of connecting to a shared printer.

Not configured - Only Administrators can install a printer driver as part of connecting to a shared printer.

Restrict CD-ROM access to local active user

Default: Not configured

CSP: Devices_RestrictCDROMAccessToLocallyLoggedOnUserOnly

Enabled - Only the interactively logged-on user can use the CD-ROM media. If this policy is enabled, and no one is logged on interactively, then the CD-ROM is accessed over the network.

Not configured - Anyone has access to the CD-ROM.

Format and eject removable media

Default: Administrators

CSP: Devices_AllowedToFormatAndEjectRemovableMedia

Define who is allowed to format and eject removable NTFS media:

Not configured

Administrators

Administrators and Power Users

Administrators and Interactive Users

Interactive Logon

Minutes of lock screen inactivity until screen saver activates

Default: Not configured

LocalPoliciesSecurityOptions CSP: InteractiveLogon_MachineInactivityLimit

Enter the maximum minutes of inactivity on the interactive desktop's sign-in screen until the screen saver starts. (0 - 99999)

Require CTRL+ALT+DEL to log on

Default: Not configured

LocalPoliciesSecurityOptions CSP: InteractiveLogon_DoNotRequireCTRLALTDEL

Enable - Pressing CTRL+ALT+DEL isn't required for users to sign in.

Not configured Require users to press CTRL+ALT+DEL before logging on to Windows.

Smart card removal behavior

Default: Lock workstation

LocalPoliciesSecurityOptions CSP: InteractiveLogon_SmartCardRemovalBehavior

Determines what happens when the smart card for a logged-on user is removed from the smart card reader. Your options:

Lock Workstation - The workstation is locked when the smart card is removed. This option allows users to leave the area, take their smart card with them, and still maintain a protected session.

No action

Force Logoff - The user is automatically logged off when the smart card is removed.

Disconnect if a Remote Desktop Services session - Removal of the smart card disconnects the session without logging off the user. This option allows the user to insert the smart card and resume the session later, or at another smart card reader-equipped computer, without having to sign in again. If the session is local, this policy functions identically to Lock Workstation.

Display

User information on lock screen

Default: Not configured

LocalPoliciesSecurityOptions CSP: InteractiveLogon_DisplayUserInformationWhenTheSessionIsLocked

Configure the user information that is displayed when the session is locked. If not configured, user display name, domain, and username are shown.

Not configured

User display name, domain, and user name

User display name only

Do not display user information

Hide last signed-in user

Default: Not configured

LocalPoliciesSecurityOptions CSP: InteractiveLogon_DoNotDisplayLastSignedIn

Enable - Hide the username.

Not configured - Show the last username.

Hide username at sign-in Default: Not Configured

LocalPoliciesSecurityOptions CSP: InteractiveLogon_DoNotDisplayUsernameAtSignIn

Enable - Hide the username.

Not configured - Show the last username.

Logon message title

Default: Not configured

LocalPoliciesSecurityOptions CSP: InteractiveLogon_MessageTitleForUsersAttemptingToLogOn

Set the message title for users signing in.

Logon message text

Default: Not configured

LocalPoliciesSecurityOptions CSP: InteractiveLogon_MessageTextForUsersAttemptingToLogOn

Set the message text for users signing in.

Network access and security

Anonymous access to Named Pipes and Shares

Default: Not configured

LocalPoliciesSecurityOptions CSP:
NetworkAccess_RestrictAnonymousAccessToNamedPipesAndShares

Not configured - Restrict anonymous access to share and Named Pipe settings. Applies to the settings that can be accessed anonymously.

Block - Disable this policy, making anonymous access available.

Anonymous enumeration of SAM accounts

Default: Not configured

LocalPoliciesSecurityOptions CSP:
NetworkAccess_DoNotAllowAnonymousEnumerationOfSAMAccounts

Not configured - Anonymous users can enumerate SAM accounts.

Block - Prevent anonymous enumeration of SAM accounts.

Anonymous enumeration of SAM accounts and shares

Default: Not configured

LocalPoliciesSecurityOptions CSP:
NetworkAccess_DoNotAllowAnonymousEnumerationOfSamAccountsAndShares

Not configured - Anonymous users can enumerate the names of domain accounts and network shares.

Block - Prevent anonymous enumeration of SAM accounts and shares.

LAN Manager hash value stored on password change

Default: Not configured

LocalPoliciesSecurityOptions CSP:
NetworkSecurity_DoNotStoreLANManagerHashValueOnNextPasswordChange

Determine if the hash value for passwords is stored the next time the password is changed.

Not configured - The hash value isn't stored

Block - The LAN Manager (LM) stores the hash value for the new password.

PKU2U authentication requests

Default: Not configured

LocalPoliciesSecurityOptions CSP: NetworkSecurity_AllowPKU2UAuthenticationRequests

Not configured- Allow PU2U requests.

Block - Block PKU2U authentication requests to the device.

Restrict remote RPC connections to SAM

Default: Not configured

LocalPoliciesSecurityOptions CSP: NetworkAccess_RestrictClientsAllowedToMakeRemoteCallsToSAM

Not configured - Use the default security descriptor, which may allow users and groups to make remote RPC calls to the SAM.

Allow - Deny users and groups from making remote RPC calls to the Security Accounts Manager (SAM), which stores user accounts and passwords. Allow also lets you change the default Security Descriptor Definition Language (SDDL) string to explicitly allow or deny users and groups to make these remote calls.

Security descriptor

Default: Not configured

Minimum Session Security For NTLM SSP Based Clients

Default: None

LocalPoliciesSecurityOptions CSP: NetworkSecurity_MinimumSessionSecurityForNTLMSSPBasedClients

This security setting allows a server to require the negotiation of 128-bit encryption and/or NTLMv2 session security.

None

Require NTLMv2 session security

Require 128-bit encryption

NTLMv2 and 128-bit encryption

Minimum Session Security For NTLM SSP Based Server

Default: None

LocalPoliciesSecurityOptions CSP: NetworkSecurity_MinimumSessionSecurityForNTLMSSPBasedServers

This security setting determines which challenge/response authentication protocol is used for network logons.

None

Require NTLMv2 session security

Require 128-bit encryption

NTLMv2 and 128-bit encryption

LAN Manager Authentication Level

Default: LM and NTLM

LocalPoliciesSecurityOptions CSP: NetworkSecurity_LANManagerAuthenticationLevel

LM and NTLM

LM, NTLM and NTLMv2

NTLM

NTLMv2

NTLMv2 and not LM

NTLMv2 and not LM or NTLM

Insecure Guest Logons

Default: Not configured

LanmanWorkstation CSP: LanmanWorkstation

If you enable this setting, the SMB client will reject insecure guest logons.

Not configured

Block - The SMB client rejects insecure guest logons.

Recovery console and shutdown

Clear virtual memory pagefile when shutting down

Default: Not configured

LocalPoliciesSecurityOptions CSP: Shutdown_ClearVirtualMemoryPageFile

Enable - Clear the virtual memory pagefile when the device is powered down.

Not configured - Doesn't clear the virtual memory.

Shut down without log on

Default: Not configured

LocalPoliciesSecurityOptions CSP: Shutdown_AllowSystemToBeShutDownWithoutHavingToLogOn

Block - Hide the shutdown option on the Windows sign in screen. Users must sign in to the device, and then shut down.

Not configured - Allow users to shut down the device from the Windows sign in screen.

User account control

UIA integrity without secure location

Default: Not Configured

LocalPoliciesSecurityOptions CSP: UserAccountControl_OnlyElevateUIAccessApplicationsThatAreInstalledInSecureLocations

Block - Apps that are in a secure location in the file system will run only with UIAccess integrity.

Not configured - Enables apps to run with UIAccess integrity, even if the apps aren't in a secure location in the file system.

Virtualize file and registry write failures to per-user locations

Default: Not Configured

LocalPoliciesSecurityOptions CSP: UserAccountControl_VirtualizeFileAndRegistryWriteFailuresToPerUserLocations

Enabled - Applications that write data to protected locations fail.

Not configured - Application write failures are redirected at run time to defined user locations for the file system and registry.

Only elevate executable files that are signed and validated

Default: Not Configured

LocalPoliciesSecurityOptions CSP: UserAccountControl_OnlyElevateUIAccessApplicationsThatAreInstalledInSecureLocations

Enabled - Enforce the PKI certification path validation for an executable file before it can run.

Not configured - Don't enforce PKI certification path validation before an executable file can run.

UIA elevation prompt behavior

Elevation prompt for admins

Default: Prompt for consent for non-Windows binaries

LocalPoliciesSecurityOptions CSP:
UserAccountControl_BehaviorOfTheElevationPromptForAdministrators

Define the behavior of the elevation prompt for admins in Admin Approval Mode.

Not configured

Elevate without prompting

Prompt for credentials on the secure desktop

Prompt for credentials

Prompt for consent

Prompt for consent for non-Windows binaries

Elevation prompt for standard users

Default: Prompt for credentials

LocalPoliciesSecurityOptions CSP:
UserAccountControl_BehaviorOfTheElevationPromptForStandardUsers

Define the behavior of the elevation prompt for standard users.

Not configured

Automatically deny elevation requests

Prompt for credentials on the secure desktop

Prompt for credentials

Route elevation prompts to user's interactive desktop

Default: Not Configured

LocalPoliciesSecurityOptions CSP:
UserAccountControl_SwitchToTheSecureDesktopWhenPromptingForElevation

Enabled - All elevation requests to go to the interactive user's desktop rather than the secure desktop. Any prompt behavior policy settings for administrators and standard users are used.

Not configured - Force all elevation requests go to the secure desktop, regardless of any prompt behavior policy settings for administrators and standard users.

Elevated prompt for app installations

Default: Not Configured

LocalPoliciesSecurityOptions CSP: UserAccountControl_DetectApplicationInstallationsAndPromptForElevation

Enabled - Application installation packages aren't detected or prompted for elevation.

Not configured - Users are prompted for an administrative user name and password when an application installation package requires elevated privileges.

UIA elevation prompt without secure desktop

Default: Not Configured

LocalPoliciesSecurityOptions CSP: UserAccountControl_AllowUIAccessApplicationsToPromptForElevation

Enable - Allow UIAccess apps to prompt for elevation, without using the secure desktop.

Not configured - Elevation prompts use a secure desktop.

Admin Approval Mode

Admin Approval Mode For Built-in Administrator

Default: Not Configured

LocalPoliciesSecurityOptions CSP: UserAccountControl_UseAdminApprovalMode

Enabled - Allow the built-in Administrator account to use Admin Approval Mode. Any operation that requires elevation of privilege prompts the user to approve the operation.

Not configured - runs all apps with full admin privileges.

Run all admins in Admin Approval Mode

Default: Not Configured

LocalPoliciesSecurityOptions CSP: UserAccountControl_RunAllAdministratorsInAdminApprovalMode

Enabled- Enable Admin Approval Mode.

Not configured - Disable Admin Approval Mode and all related UAC policy settings.

Microsoft Network Client

Digitally sign communications (if server agrees)

Default: Not configured

LocalPoliciesSecurityOptions CSP: MicrosoftNetworkClient_DigitallySignCommunicationsIfServerAgrees

Determines if the SMB client negotiates SMB packet signing.

Block - The SMB client never negotiates SMB packet signing.

Not configured - The Microsoft network client asks the server to run SMB packet signing upon session setup. If packet signing is enabled on the server, packet signing is negotiated.

Send unencrypted password to third-party SMB servers

Default: Not configured

LocalPoliciesSecurityOptions CSP: MicrosoftNetworkClient_SendUnencryptedPasswordToThirdPartySMBServers

Block - The Server Message Block (SMB) redirector can send plaintext passwords to non-Microsoft SMB servers that don't support password encryption during authentication.

Not configured - Block sending of plaintext passwords. The passwords are encrypted.

Digitally sign communications (always)

Default: Not configured

LocalPoliciesSecurityOptions CSP: MicrosoftNetworkClient_DigitallySignCommunicationsAlways

Enable - The Microsoft network client doesn't communicate with a Microsoft network server unless that server agrees to SMB packet signing.

Not configured - SMB packet signing is negotiated between the client and server.

Microsoft Network Server

Digitally sign communications (if client agrees)

Default: Not configured

CSP: MicrosoftNetworkServer_DigitallySignCommunicationsIfClientAgrees

Enable - The Microsoft network server negotiates SMB packet signing as requested by the client. That is, if packet signing is enabled on the client, packet signing is negotiated.

Not configured - The SMB client never negotiates SMB packet signing.

Digitally sign communications (always)

Default: Not configured

CSP: MicrosoftNetworkServer_DigitallySignCommunicationsAlways

Enable - The Microsoft network server doesn't communicate with a Microsoft network client unless that client agrees to SMB packet signing.

Not configured - SMB packet signing is negotiated between the client and server.

Xbox services

Xbox Game Save Task

Default: Not configured

CSP: TaskScheduler/EnableXboxGameSaveTask

This setting determines whether the Xbox Game Save Task is Enabled or Disabled.

Enabled

Not configured

Xbox Accessory Management Service

Default: Manual

CSP: SystemServices/ConfigureXboxAccessoryManagementServiceStartupMode

This setting determines the Accessory Management Service's start type.

Manual

Automatic

Disabled

Xbox Live Auth Manager Service

Default: Manual

CSP: SystemServices/ConfigureXboxLiveAuthManagerServiceStartupMode

This setting determines the Live Auth Manager Service's start type.

Manual

Automatic

Disabled

Xbox Live Game Save Service

Default: Manual

CSP: SystemServices/ConfigureXboxLiveGameSaveServiceStartupMode

This setting determines the Live Game Save Service's start type.

Manual

Automatic

Disabled

Xbox Live Networking Service

Default: Manual

CSP: SystemServices/ConfigureXboxLiveNetworkingServiceStartupMode

This setting determines the Networking Service's start type.

Manual

Automatic

Disabled

Next steps

The profile is created, but it's not doing anything yet. Next, assign the profile, and monitor its status.

Configure endpoint protections settings on macOS devices.