

# Operational and Administrative Guidance

## Microsoft Windows 10 and Windows Server

Version 5.0, January 16, 2020

Common Criteria Evaluation for  
Microsoft Windows 10 and Windows Server  
Version 1909

General Purpose Operating System Protection Profile



## Copyright and disclaimer

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. This work is licensed under the Creative Commons Attribution-NoDerivs-NonCommercial VLicense (which allows redistribution of the work). To view a copy of this license, visit <http://creativecommons.org/licenses/by-nd-nc/1.0/> or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2020 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, Visual Basic, Visual Studio, Windows, the Windows logo, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



# Microsoft Windows 10 GP OS Administrative Guidance

1	Contents	
2	Change history .....	9
3	Introduction.....	10
3.1	What's new.....	10
3.2	How this guide is organized.....	10
3.3	Links to other resources.....	11
3.4	Security Target document.....	11
3.5	Guidance specific to user roles .....	11
3.6	Modern device management.....	13
3.7	Approaches for configuring Windows policies .....	14
3.7.1	Setting policies with modern device management (MDM):.....	14
3.7.2	Setting policies with Group Policy Objects (GPO):.....	14
3.7.3	Setting policies with PowerShell and Group Policy Objects:.....	15
4	Evaluated editions and platforms .....	16
5	Evaluated configuration.....	17
5.1	Installing the operating system.....	17
5.2	Operational prerequisites.....	18
5.2.1	Trusted platforms .....	18
5.2.2	Device administration .....	18
5.2.3	Security updates.....	18
5.2.4	Mode of operation.....	19
5.2.5	FIPS 140 Approved cryptography mode.....	19
5.2.6	Additional cryptography configuration.....	21
5.2.7	Code integrity configuration .....	21
5.2.8	Device access configuration .....	22
6	Managing evaluated features.....	23



## Microsoft Windows 10 GP OS Administrative Guidance

6.1	Managing cryptography .....	23
6.2	Managing X.509 certificates .....	24
6.2.1	Client certificates and Certificate Authorities.....	24
6.2.2	Trusted root certificates .....	26
6.2.3	Certificate name comparison .....	27
6.2.4	Certificate validation and revocation check.....	28
6.3	Managing Transport Layer Security (TLS).....	30
6.3.1	Available TLS ciphersuites .....	30
6.3.2	Available EAP-TLS ciphersuites.....	31
6.3.3	Configuring with MDM.....	32
6.3.4	Configuring with PowerShell .....	32
6.3.5	Configuring with group policy.....	33
6.3.6	Configuring key establishment schemes.....	34
6.3.7	Managing signature algorithms with the Windows registry .....	35
6.3.8	Choosing TLS in a web browser .....	35
6.4	Managing IPsec and VPN connections .....	36
6.4.1	Configuring IPsec firewall rules using Windows Defender Firewall with Advanced Security.....	36
6.4.2	Configuring and using VPN connections and the VPN client .....	40
6.4.3	Configuring security association (SA) parameters .....	45
6.5	Managing network connections .....	48
6.5.1	Enabling or disabling network connections with the Windows UI .....	48
6.5.2	Enabling or disabling network connections with PowerShell .....	49
6.5.3	Configuring Wi-Fi access with MDM.....	49
6.5.4	Configuring Wi-Fi access with the Windows user interface .....	50
6.5.5	Configuring allowed Wi-Fi networks with MDM .....	50



## Microsoft Windows 10 GP OS Administrative Guidance

6.5.6	Configuring allowed Wi-Fi networks with Group Policy .....	51
6.5.7	Selecting a secure Wi-Fi connection with the Windows UI .....	51
6.5.8	Configuring a Wi-Fi connection profile with the Windows UI .....	52
6.6	Managing personal hotspots .....	53
6.6.1	Configuring with MDM .....	53
6.6.2	Configuring with group policy .....	54
6.6.3	Configuring with the Windows user interface .....	54
6.7	Managing Bluetooth .....	55
6.7.1	Configuring Bluetooth adapters with MDM .....	55
6.7.2	Configuring Bluetooth properties with MDM .....	55
6.7.3	Enabling or disabling Bluetooth adapters via Device Manager .....	56
6.7.4	Enabling or disabling Bluetooth adapters with PowerShell .....	56
6.7.5	Pairing Bluetooth devices with the Windows UI .....	57
6.8	Managing passwords and password policy .....	57
6.8.1	Configuring with MDM .....	57
6.8.2	Configuring with group policy .....	59
6.8.3	Configuring with net.exe accounts utility .....	60
6.9	Managing smart card logon .....	61
6.10	Managing Windows Hello .....	62
6.10.1	Configuring biometric authentication with the Windows UI .....	62
6.10.2	Configuring Windows Hello for Business with group policy or MDM .....	62
6.10.3	Configuring PIN authentication with the Windows UI .....	63
6.11	Managing screen lock and session timeout .....	64
6.11.1	Configuring with MDM .....	64
6.11.2	Configuring with group policy .....	64
6.11.3	Configuring with the Windows registry .....	65



## Microsoft Windows 10 GP OS Administrative Guidance

6.11.4	Transitioning to the locked state with the Windows user interface .....	65
6.12	Managing the logon banner .....	66
6.12.1	Configuring with MDM .....	66
6.12.2	Configuring with group policy .....	66
6.12.3	Configuring with the Windows registry .....	67
6.13	Managing USB .....	67
6.13.1	Configuring via Device Manager .....	67
6.13.2	Configuring with PowerShell .....	68
6.13.3	Configuring with the Windows registry .....	68
6.14	Managing updates .....	69
6.14.1	Configuring using MDM .....	69
6.14.2	Configuring using group policy .....	70
6.14.3	Configuring using the Server Configuration tool .....	70
6.14.4	Checking for OS updates using the Windows UI .....	71
6.14.5	Querying for Windows version and hardware information .....	71
6.14.6	Installing Windows updates via the command line .....	72
6.14.7	Checking for Windows Store application updates .....	72
6.14.8	Querying for installed application version information .....	73
6.15	Managing diagnostic data .....	73
6.15.1	Configuring with group policy .....	73
6.15.2	Configuring with MDM .....	74
6.15.3	Configuring with the Windows UI .....	75
6.16	Managing the firewall .....	75
6.16.1	Configuring with PowerShell .....	75
6.17	Managing domains .....	76
6.17.1	Configuring with PowerShell .....	76



## Microsoft Windows 10 GP OS Administrative Guidance

6.18	Managing date and time .....	76
6.18.1	Configuring with PowerShell.....	76
6.18.2	Configuring with Windows Time Service Tools .....	77
6.18.3	Configuring with the Windows user interface.....	77
6.19	Managing remote administration .....	78
6.19.1	Configuring with MDM .....	78
6.19.2	Configuring with group policy .....	79
6.19.3	Configuring with PowerShell.....	79
6.20	Managing apps and software restriction policies .....	79
6.20.1	Configuring with Windows Defender Application Control.....	80
6.20.2	Configuring with AppLocker .....	80
6.20.3	Configuring with enterprise app management and MDM.....	81
6.20.4	Installing and uninstalling apps with the Windows user interface .....	82
6.21	Developing applications .....	83
6.22	Managing self-test and health attestation.....	83
6.22.1	Configuring with MDM .....	83
6.22.2	Helper utility for health attestation logs .....	84
6.23	Managing audit policy.....	84
6.23.1	Managing audit policy with the Auditpol command.....	85
6.23.2	Managing audit policy with the Secpol snap-in.....	86
6.23.3	Managing audit policy with the Wevtutil utility .....	87
6.23.4	Retrieving and viewing audit logs using Get-WinEvent.....	87
6.23.5	Configuring System Access Control Lists for audited objects.....	87
7	Audit events .....	89
7.1	Audit events – GP OS protection profile .....	89
7.2	Audit events – WLAN client extended package.....	91



## Microsoft Windows 10 GP OS Administrative Guidance

7.3	Audit events – IPsec Extended Package.....	93
7.4	Events mapped to log details .....	96
8	Configuration Annex.....	113
8.1	Supported Configuration Actions .....	113
8.1.1	Logon banner text.....	117



## 2 Change history

---

Version	Date	Description
1.0	March 20, 2018	Administrative Guide for Windows 10 and Windows Server Fall Creators Update (1709)
2.0	October 11, 2018	Administrative Guide for Windows 10 and Windows Server April 2018 Update (1803)
3.0	February 21, 2019	Administrative Guide for Windows 10 and Windows Server 2019, Version 1809 (October 2018 Update)
4.0	June 10, 2019	Administrative Guide for Windows 10 and Windows Server, Version 1903 (May 2019 Update)
5.0	January 16, 2020	Administrative Guide for Windows 10 and Windows Server, Version 1909



## 3 Introduction

---

This administrative guide provides information for Windows 10 and Windows Server, version 1909, as required by the Common Criteria General Purpose Operating System (GP OS) protection profile. All Windows 10 editions may be referred to collectively as “Windows” where appropriate. The goals of this administrative guide are to enable an IT professional to configure Windows and its operational environment to match the configuration under which the product was evaluated and to manage the Windows features in the scope of evaluation. The audience of this document is an IT Administrator familiar with current administrative practices for Windows 10. IT Administrators must follow the guidance in this document to ensure a device matches the evaluated configuration.

### 3.1 What’s new

The substantive changes in this administrative guide since the last evaluation of Windows 10 and Windows Server against the Common Criteria GP OS protection profile include:

- The scope of certification has grown to include the IPsec Extended Package and the administrative guide has been updated to match. IPsec content is integrated in the guide near related non-IPsec content.

### 3.2 How this guide is organized

The sections in this administrative guide group information together categorically:

- Section 3, [Introduction](#), provides an overview of the guide, explains conventions in the document, and includes general guidance that the subsequent sections may refer back to.
- Section 4, [Evaluated editions and platforms](#), identifies the specific editions of Windows 10 and Windows Server that were evaluated and the set of hardware platforms the evaluation was performed on.
- Section 5, [Evaluated configuration](#), covers deployment of the product and the set of operational prerequisites and configuration choices that must be followed to match the evaluated Windows configuration.




## Microsoft Windows 10 GP OS Administrative Guidance

- Section 6, [Managing evaluated features](#), covers management of the Windows features in the scope of evaluation. This includes guidance on relevant feature configuration choices and approaches to implementing them, organized by feature area.
- Section 7, [Audit events](#), provides detailed information on the audit events relevant to the evaluated configuration that are available in Windows logs. This information enables administrators to perform security monitoring and forensics.

### 3.3 Links to other resources

This document provides many external links to public Microsoft resources for additional information or detailed instructions.

 **Note:** Some external links may have originally been authored for earlier versions of Windows, e.g. Windows 8.x. In all cases, the information also applies to the evaluated version.

### 3.4 Security Target document

The Common Criteria evaluation requires a Security Target document that outlines the evaluation scope, which this guide may refer to. The correct matching Security Target for this administrative guide is the Microsoft Windows 10, Windows Server version 1909 Security Target and is available on the following sites:

- Microsoft publishes all Common Criteria evaluation documentation at <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-platform-common-criteria>.
- The worldwide Common Criteria Recognition Arrangement portal provides Security Targets for all certified products at <https://www.commoncriteriaportal.org/products/>.

### 3.5 Guidance specific to user roles

This administrative guide identifies what user role guidance is targeted at. The evaluated configuration includes three Windows user roles:



## Microsoft Windows 10 GP OS Administrative Guidance

- IT Administrator – a remote administrator using Modern device Management (MDM), Group Policy Objects (GPO), or other remote solutions to administer Windows.
- Local Administrator – a local user account that is a member of the local Administrators group. The solutions provided for local administrators include command-line utilities, Windows PowerShell cmdlets, the Windows registry, and features in the Windows graphical user interface that are only accessible to administrators.
- Standard User – a local user account that is not a member of the local Administrators group. The solutions provided for standard users are all features within the Windows graphical user interface.

Where appropriate, this administrative guide provides different configuration instructions for each user role. In the introduction of each section that provides specific guidance, a summary table like the following identifies which role the guidance is targeted at:

<b>Role</b>	IT Administrator Local Administrator Standard User
-------------	--

Access to user-accessible functions is controlled by the rights and privileges assigned to these user roles. No additional measures are needed to control access to the user-accessible functions in a secure processing environment. Attempts to access user-accessible functions that require local administrator rights or privileges are denied for the user role.

The following articles describe local accounts in Windows and how to make a standard user account a member of the local Administrators group:


- Local accounts: <https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts>
- Add a member to a local group: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524\(v%3dws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524(v%3dws.11))



## 3.6 Modern device management


<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

The evaluation was performed both with devices enrolled in modern device management (MDM) and with devices not enrolled in MDM. Where appropriate, this administrative guide provides configuration instructions specific to the management function for IT Administrators using MDM to administer devices. This guide will refer to specific Configuration Service Providers (CSPs) that enable MDM to affect a given management function.

 **Note:** MDM may not be used to manage Windows Server editions.

The following articles provide general information on using MDM to administer Windows, including solutions for enrolling and unenrolling (disconnecting) devices:

- Introducing MDM for administering Windows 10 and Windows Server devices: <https://docs.microsoft.com/en-us/windows/client-management/mdm/>
- Enrolling Windows devices for MDM: <https://docs.microsoft.com/en-us/windows/client-management/mdm/mdm-enrollment-of-windows-devices>
- Disconnecting from the management infrastructure (unenrollment): <https://docs.microsoft.com/en-us/windows/client-management/mdm/disconnecting-from-mdm-unenrollment>

 **Note:** MDM solutions may also have prerequisites for enrollment, for example trusting the MDM certificate. Guidance for MDM prerequisites are out of scope of this documentation. IT Administrators should consult the MDM documentation to make sure that prerequisites are understood and met before enrollment is performed.



## 3.7 Approaches for configuring Windows policies

Multiple sections of this guide refer to Windows policies. This section outlines different approaches administrators may take to configure and deploy policies. Use the approach that best fits the Windows edition and operational environment.

### 3.7.1 Setting policies with modern device management (MDM):

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

Policies may be configured remotely by an IT Administrator using an MDM solution and Windows Configuration Service Providers (CSPs). This guide references specific CSPs and functions within them as solutions that may be used with different MDM systems. See the MDM solution documentation for detailed configuration actions. The following articles provide a reference to Windows CSPs and details on the Policy CSP, which includes many of the solutions detailed in this guide:

- Configuration Service Provider Reference - <https://docs.microsoft.com/en-us/windows/client-management/mdm/configuration-service-provider-reference>
- Policy Configuration Service Provider - <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider>.


### 3.7.2 Setting policies with Group Policy Objects (GPO):

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter



## Microsoft Windows 10 GP OS Administrative Guidance

Group policy may be used to set Windows policies for domain-joined machines. Policies are configured using the Group Policy Editor (gpedit.msc) or Local Security Policy Editor (secpol.msc).

 **Note:** The policy editing tools are not available on Windows 10 Home Edition. For Windows 10 Home Edition enable policies by other means, e.g. PowerShell commands or the Windows user interface.

Group Policy Editor may also be used to remotely administrate policy on a machine by following these steps:

1. **Start > Run > mmc**
2. **File > Add/Remove Snap-in**
3. Under the **Standalone** tab, click **Add...**
4. Choose **Group Policy Object Editor**
5. In the following wizard, click the **Browse** button
6. Click the **Computers** tab, select the **Another Computer** radio button, and type the name of the computer or browse to it.
7. Click **OK**, then **Finish**, then **Close**, and finally **OK** again.

### 3.7.3 Setting policies with PowerShell and Group Policy Objects:

<b>Role</b>	IT Administrator, Local Administrator
<b>Windows Editions</b>	All

Group policies may also be set with PowerShell scripts. The following article provides an overview of the PowerShell cmdlets available to do this:

- GroupPolicy: <https://docs.microsoft.com/en-us/powershell/module/grouppolicy/?view=win10-ps>

Here is an example PowerShell script to enable the FIPS cryptography mode, which is one of the operational prerequisites for the evaluated configuration. To enable this policy, run the PowerShell script on the target machine.



```
Enable "System cryptography: Use FIPS 140...":  
Set-ItemProperty -Path Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy -  
Name Enabled -Value "1"
```

## 4 Evaluated editions and platforms

---

This administrative guide applies to the following Windows operating system (OS) editions, each of which was tested as part of the evaluated configuration:

- Microsoft Windows 10 Home edition (version 1909) (32-bit and 64-bit versions)
- Microsoft Windows 10 Pro edition (version 1909) (64-bit version)
- Microsoft Windows 10 Enterprise edition (version 1909) (64-bit version)
- Microsoft Windows Server Standard edition, version (version 1909)
- Microsoft Windows Server Datacenter edition, version (version 1909)

In the introduction of each section that provides specific guidance, a summary table like the following identifies which Windows editions the guidance applies to:

Windows Editions	Pro, Enterprise, Server Standard
------------------	----------------------------------

The Common Criteria evaluation was performed on the following hardware platforms:

- Microsoft Surface Go
- Microsoft Surface Go LTE
- Microsoft Surface Pro LTE
- Microsoft Surface Book 2
- Microsoft Surface Pro 6
- Microsoft Surface Laptop 2
- Microsoft Surface Studio 2



- Microsoft Windows Server 2019 Hyper-V
- Microsoft Windows Server 2016 Hyper-V
- Dell Latitude 7200 2-in-1
- Dell Latitude 5300 2-in-1
- Dell PowerEdge R740
- Dell PowerEdge R7425
- HPZBook 15G6
- HP EliteBook x360 650G5
- Panasonic Toughbook CF-33
- Samsung Galaxy Book 10.6"
- Samsung Galaxy Book 12"

## 5 Evaluated configuration

---

This section provides guidance on deploying the operating system and meeting the prerequisites for operating Windows 10 and Windows Server in the evaluated configuration. To operate the system in a secure state, administrators must utilize the guidance in this section and in subsequent sections, where applicable to the local environment, to administer devices.

### 5.1 Installing the operating system

The operating system may be pre-installed on the devices in the evaluated configuration. When the device is turned on for the first time the Out of Box Experience (OOBE) runs to complete the initial configuration.

The operating system may also be installed from installation media. The method for creating or obtaining installation media depends on the Windows edition.

- For all editions except Enterprise, the following article includes procedures to download installation media as an ISO file for installation, create bootable media using the ISO file, and install the operating system:



Download Windows 10: <https://www.microsoft.com/en-us/software-download/windows10>

- For Windows 10 Enterprise edition, installation media must be obtained through Volume Licensing.

## 5.2 Operational prerequisites

The following operational prerequisites are required to operate Windows 10 and Windows Server in the evaluated configuration.

### 5.2.1 Trusted platforms

Windows 10 and Windows Server must be installed on trusted hardware platforms to ensure a secure operating state. See section 4, [Evaluated editions and platforms](#), for details on which hardware platforms the evaluation was performed on.

### 5.2.2 Device administration

Users must use a separate account that is a member of the local Administrators group to perform the procedures in sections of this document tagged with “Local Administrator” or set the device up for IT administration. For Windows 10, IT administration is joining the device to a Windows domain or enrolling the device for modern device management (MDM) to receive MDM policies. For Windows Server IT administration is joining the device to a Windows domain to receive domain group policy.

### 5.2.3 Security updates

For this evaluation, Windows 10 and Windows Server was evaluated with all critical updates available as of October 31, 2019 installed. See section 1 of the Security Target for related information. The current list of updates for this version of Windows and a description of the differences between it and previous releases are included in the release notes, available at <https://support.microsoft.com/en-us/help/4529964/windows-10-update-history>.



### 5.2.4 Mode of operation

Windows 10 and Windows Server have four modes of operation, as listed below. The evaluated configuration for Windows is the Operational Mode.

- Operational Mode – The normal mode of operation when the system has booted. This is the only evaluated mode.
- Debug Mode – The mode where the Windows boot options are configured to enable kernel debugging of the operating system.
- Safe Mode – The mode where Windows boot options are configured to start the operating system in a limited state where only essential programs are loaded.
- Non-Operational Mode – The mode where the system has not booted normally. In this mode the system is not operational and must be reinstalled.

### 5.2.5 FIPS 140 Approved cryptography mode

To match the evaluated configuration, Windows cryptography must be placed into the FIPS 140 Approved cryptography mode. This leverages FIPS 140 compliant cryptographic algorithms, including encryption, hashing, and signing algorithms. See the following article for more information on FIPS 140 mode:

- System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/system-cryptography-use-fips-compliant-algorithms-for-encryption-hashing-and-signing>

#### 5.2.5.1 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

Setting FIPS 140 mode may be configured by an IT Administrator using MDM and the Cryptography function of the Policy CSP. See



## Microsoft Windows 10 GP OS Administrative Guidance

the MDM solution documentation for detailed management actions. The following article provides information on the Cryptography function of the Policy CSP:

- Policy CSP – Cryptography <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-cryptography>

### 5.2.5.2 Configuring with Group Policy

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Setting FIPS 140 mode may be configured using Group Policy. Specifically, enable the following security policy:

Security Policy	Policy Setting
<b>Local Policies\Security Options\System cryptography:</b> Use FIPS 140 compliant cryptographic algorithms, including encryption, hashing and signing algorithm	Enabled

For general information on how to set policies in Windows, see the section, [Setting policies with Group Policy Objects \(GPO\)](#). For additional encryption configuration details beyond this operational prerequisite, see the section, [Managing Transport Layer Security \(TLS\)](#).

### 5.2.5.3 Configuring with the Windows Registry

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	All



To set FIPS mode, make the following change to the Windows registry:

Registry Node	Setting
HKLM\System\CurrentControlSet\Control\Lsa\FIPSAAlgorithmPolicy\Enabled	1

### 5.2.6 Additional cryptography configuration

In addition to enabling FIPS 140 mode, the following specific configuration guidance must be followed:

- Cipher suite selection must be configured according to section 6.3, [Managing Transport Layer Security \(TLS\)](#).
- When Windows is configured to use TLS 1.2, SHA1 algorithms should be prioritized at the bottom of the algorithm negotiation list. See section 6.3, [Managing Transport Layer Security \(TLS\)](#), for implementation guidance.
- RSA machine certificates must be configured with templates to use a minimum 2048-bit key length. See section 6.2, [Managing X.509 certificates](#), for implementation guidance.

### 5.2.7 Code integrity configuration

The evaluated configuration enforces an example code integrity policy using Windows Defender Application Control (WDAC) that protects the integrity of executable code relevant to different evaluation requirements. With this policy, any violations of code integrity for those executables are recorded in auditable log events (#3033, #3076, and #3077, as documented in [Audit events](#)). This policy, included with Windows, is intended as a starting point for administrators. Administrators should modify the policy as appropriate for the operational environment and to allow approved apps to run. Once modified, administrators may establish the policy using WDAC PowerShell commands and may distribute it locally or remotely via Group Policy. The steps below outline the procedure to establish and enable the unmodified example policy on a local machine.

- Start an elevated PowerShell command window.



## Microsoft Windows 10 GP OS Administrative Guidance

- Navigate to the directory where the Windows code integrity example policies are located:

```
PS C:\> cd "windows\schemas\CodeIntegrity\ExamplePolicies"
```

- Convert the DefaultWindows\_Audit\_Enforced.xml policy to a binary form with the specific binary filename listed below:

```
PS C:\windows\schemas\CodeIntegrity\ExamplePolicies> convertFrom-CIPolicy -XmlFilePath  
".\DefaultWindows_Audit_Enforced.xml" -BinaryFilePath ".\{A244370E-44C9-4C06-B551-F6016E563076}.cip"
```

- Copy the binary policy to C:\Windows\System32\CodeIntegrity\CiPolicies\Active:

```
PS C:\windows\schemas\CodeIntegrity\ExamplePolicies> cp ".\{A244370E-44C9-4C06-B551-F6016E563076}.cip"  
C:\Windows\System32\CodeIntegrity\CiPolicies\Active
```

- Restart the machine to apply the policy.

The following topics provide additional reference information on enforcing and deploying WDAC policies:

- Enforce Windows Defender Application Control policies: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/enforce-windows-defender-application-control-policies>
- Deploy Windows Defender Application Control policies by using Group Policy: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/deploy-windows-defender-application-control-policies-using-group-policy>

### 5.2.8 Device access configuration

The following configuration guidance must be followed to ensure device access is secured.

- Complex passwords must be required. See section 6.8, [Managing passwords and password policy](#), for implementation guidance.
- The password reveal button must be disabled. See section 6.8, [Managing passwords and password policy](#), for implementation guidance.
- Session locking must be enabled. See section 6.11, [Managing screen lock and session timeout](#), for implementation guidance.



## 6 Managing evaluated features

---

This section provides management information for the features in scope for the evaluation, including configuration details and options for implementing them. Each subsection groups the information for a single feature or a group of related features.

### 6.1 Managing cryptography

Cryptography functions in Windows are managed by the Cryptography API: Next Generation (CNG). The notes below call out a list of specific management functions relevant to this Common Criteria evaluation that are handled automatically by CNG. The sections that follow in this Administrative Guide provide complementary information on managing specific cryptography functions within Windows.

#### **Notes:**

- Key management, including AES key size, storage, and destruction is handled automatically by CNG and requires no configuration. Keys are destroyed during Device Wipe.
- Windows generates asymmetric RSA keys using methods that meet FIPS-PUB 186-4 Appendix B.3, no configuration is necessary.
- Windows generates asymmetric ECC keys using methods that meet FIPS-PUB 186-4 Appendix B.4, no configuration is necessary.
- Windows performs RSA-based key establishment that meet NIST SP 800-56B, no configuration is necessary.
- Windows performs elliptic curve-based key schemes that meet NIST SP 800-56A, no configuration is necessary.
- Windows generates random numbers according to NIST SP 800-90A, no configuration is necessary.
- Unprotected keys are not stored in non-volatile memory.
- Key lengths of keys used with certificates are configured in the certificate templates on the Certificate Authority used during enrollment and are not configured by the user or local administrator.
- There is no global configuration for hashing algorithms. The use of required hash sizes is supported. No configuration is necessary.
- Cryptographic Algorithm Validation Program (CAVP) testing was performed on the system cryptographic engine. Other cryptographic engines may have been separately evaluated but were not part of this CC evaluation.



## 6.2 Managing X.509 certificates

### 6.2.1 Client certificates and Certificate Authorities

The device comes preloaded with root certificates for various Certificate Authorities. Additional Certificate Authorities may be managed on the device using the solutions detailed in the subsections below.

#### **Notes:**

- There is no configuration necessary to use client authentication on the device once a device has client authentication certificates.
- To destroy all keys on a device, including any imported, wipe the device.

#### 6.2.1.1 Configuring with the Certutil command line utility

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

The Certutil command-line utility is available to dump and display certification authority (CA) configuration information, configure Certificate Services, backup and restore CA components, and verify certificates, key pairs, and certificate chains. The following article provides more information on Certutil:

- Certutil: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil>

#### 6.2.1.2 Configuring with PowerShell

<b>Role</b>	Local Administrator
-------------	---------------------



## Microsoft Windows 10 GP OS Administrative Guidance

<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter
-------------------------	---

The PKIClient cmdlets enable a local administrator to complete a variety of tasks related to public key infrastructure (PKI), including importing a client certificate. See the following topics for more information:

- PKIClient cmdlet reference: <https://docs.microsoft.com/en-us/powershell/module/pkiclient/?view=win10-ps>
- Import-Certificate: <https://docs.microsoft.com/en-us/powershell/module/pkiclient/Import-Certificate?view=win10-ps>

### 6.2.1.3 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

Client certificates may be managed by the IT Administrator using MDM. See the MDM solution documentation for detailed management actions. The following article describes the MDM policy for client certificate management, including deleting certificates:

- ClientCertificateInstall CSP - <https://docs.microsoft.com/en-us/windows/client-management/mdm/clientcertificateinstall-csp>

### 6.2.1.4 Configuring with the Windows UI

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise

The following article describes how to manually import a certificate:



## Microsoft Windows 10 GP OS Administrative Guidance

- Import a Certificate: <http://technet.microsoft.com/en-us/library/cc754489.aspx>

The user obtains a client certificate for authentication by following the procedures in the following article:

- Obtain a Certificate: <https://technet.microsoft.com/en-us/library/cc754246.aspx>

To destroy all keys on a device, including any imported, wipe the device.

### 6.2.1.5 Configuring certificate request fields

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Certificate requests with specific fields such as "Common Name", "Organization", "Organizational Unit", and/or "Country" can be generated by apps using the `Certificates.CertificateEnrollmentManager.CreateRequestAsync` API. The following link provides the documentation for the API:

- `CertificateEnrollmentManager.CreateRequestAsync` | `createRequestAsync` method: <https://docs.microsoft.com/en-us/uwp/api/Windows.Security.Cryptography.Certificates.CertificateEnrollmentManager>

Similarly, the Network Device Enrollment Service (NDES) PowerShell cmdlet can be used to configure the same specific fields for the registration authority. The following article provides more information on installing and using NDES:

- Install-AdcsNetworkDeviceEnrollmentService: <https://docs.microsoft.com/en-us/powershell/module/adcsdeployment/install-adcsnetworkdeviceenrollmentservice?view=win10-ps>

### 6.2.2 Trusted root certificates

Windows is preloaded with trusted root certificates for several Certification Authorities (CAs). The subsections below provide solutions for additional management of trusted root certificates.



## Microsoft Windows 10 GP OS Administrative Guidance

### 6.2.2.1 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

Certificate trust relationships may be managed by the IT Administrator using MDM. See the MDM solution documentation for detailed management actions. The following article describes the CSP that enables MDM to affect the policy for trusted root certificates:

- RootCATrustedCertificates CSP: <https://docs.microsoft.com/en-us/windows/client-management/mdm/rootcacertificates-csp>

### 6.2.2.2 Configuring with group policy

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

The following article describes how to distribute certificates using group policy:

- Distribute Certificates to Client Computers by Using Group Policy: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-computers-by-using-group-policy>

### 6.2.3 Certificate name comparison


Windows automatically compares the distinguished name (DN) in the certificate to the expected distinguished name and does not require additional configuration of the expected distinguished name for the connection.



## Microsoft Windows 10 GP OS Administrative Guidance

The reference identifiers for TLS are the DNS name or IP address of the remote server, which is compared against the DNS name as the presented identifier in either the Subject Alternative Name (SAN) or the Subject Name of the certificate. There is no configuration of the reference identifiers.

### 6.2.4 Certificate validation and revocation check

 **Note:** When validating a certificate with modern Windows applications the connection to a configured revocation server must be available or the validation will fail. This configuration cannot be changed for modern applications. The content below provides information on configuring certificate validation for other scenarios.

#### 6.2.4.1 Configuring revocation lists and certificate trust lists using CertMgr

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	All

The CertMgr utility provides a local administrator the ability to manage certificate trust lists and certificate revocation lists. The following topic provides more information on CertMgr:

- CertMgr: <https://docs.microsoft.com/en-us/windows/win32/seccrypto/certmgr>

#### 6.2.4.2 Configuring certificate validation for EAP-TLS

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	All

The administrator configures certificate validation for network connections based on EAP-TLS using the “Set Up a Connection or Network” wizard. The following topic provides more information:



## Microsoft Windows 10 GP OS Administrative Guidance

- EAP configuration: <https://docs.microsoft.com/en-us/windows/client-management/mdm/eap-configuration>

### 6.2.4.3 Configuring certificate validation for HTTPS in web browsers

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	Home, Pro, Enterprise

For Internet Explorer:

- Open the **Control Panel**
- Navigate to **Internet Options > Internet Properties > Advanced Tab**
- Configure certificate validation using the checkbox options. The **Warn about certificate address mismatch** setting configures whether the Web address must match the certificate subject field and warns the user of a mismatch

The following MSDN Blog article provides more information on how Internet Explorer performs certificate revocation checks specifically:

- Understanding Certificate Revocation Checks: <https://blogs.msdn.microsoft.com/ieinternals/2011/04/07/understanding-certificate-revocation-checks/>

For Microsoft Edge: The administrator cannot configure certificate validation for HTTPS for Microsoft Edge. If the Web address does not match the certificate subject field, then the user is warned of a mismatch.

In all cases: When using HTTPS in a browsing scenario the user may choose to ignore a failed certificate validation and continue the connection.

### 6.2.4.4 Certificate validation and code signing

The administrator cannot configure certificate validation for code signing purposes.



## 6.3 Managing Transport Layer Security (TLS)

### Notes:

- All TLS settings such as cipher suites also apply to DTLS.

### 6.3.1 Available TLS ciphersuites

The ciphersuites listed in the Security Target correlate with those available in Windows 10 and Windows Server as follows:

Ciphersuites listed in the Security Target	Setting name for the ciphersuite in Windows
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246	TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246	TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246	TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246	TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288	TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288	TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384



## Microsoft Windows 10 GP OS Administrative Guidance

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

See the following article for additional information on TLS ciphersuites available in Windows 10. Note that this same set of ciphersuites applies to versions 1903 and 1909, as they share a common core operating system:

- TLS Ciphersuites in Windows 10: <https://docs.microsoft.com/en-us/windows/desktop/SecAuthN/tls-cipher-suites-in-windows-10-v1903>.

### 6.3.2 Available EAP-TLS ciphersuites

The EAP-TLS ciphersuites listed in the Security Target correlate with those available in Windows 10 and Windows Server as follows:

Ciphersuites listed in the Security Target	Setting name for the ciphersuite in Windows
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246	TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246	TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246	TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246	TLS_RSA_WITH_AES_256_CBC_SHA256



## Microsoft Windows 10 GP OS Administrative Guidance

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5430	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5430	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

The following article provides more information on ciphersuites in TLS/SSL (Schannel SSP):

- <https://docs.microsoft.com/en-us/windows/desktop/SecAuthN/cipher-suites-in-schannel>

### 6.3.3 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

TLS ciphersuite priority and restricting use of certain cryptographic algorithms may be configured by the IT Administrator using MDM. See the MDM solution documentation for detailed configuration actions. The following article describes the CSP used with MDM to set policy for TLS ciphersuites:


- Policy CSP, Cryptography/TLSCiphersuites function: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-cryptography#cryptography-tlsciphersuites>

### 6.3.4 Configuring with PowerShell

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	All




Manage TLS ciphersuites and elliptic curves using the following PowerShell cmdlets:

 **Note:** PowerShell is the recommended method to configure ciphersuites on domain-joined computers.

- [Enable-TlsCipherSuite](#)
- [Disable-TlsCipherSuite](#)
- [Enable-TlsEccCurve](#)
- [Disable-TlsEccCurve](#)


### 6.3.5 Configuring with group policy

<b>Role</b>	IT Administrator, Local Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

 **Note:** PowerShell is recommended over group policy to configure ciphersuites on domain-joined computers. See the PowerShell guidance that precedes this section.

The following articles explain how an administrator modifies the set of TLS ciphersuites for priority and availability:

- Prioritizing Schannel Ciphersuites: [https://msdn.microsoft.com/en-us/library/windows/desktop/bb870930\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/bb870930(v=vs.85).aspx)

 **Note:** The configuration for elliptic curves uses an SSL ciphersuite order list and an ECC curve order list displayed in the Group Policy Editor and the Local Security Policy Editor. Enable/order the desired ciphersuites in the first list and enable/order the elliptic curves in the second. For example, to configure only TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 ciphersuite and secp256r1 curve, edit the first list to only include TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 and the curve order list to only include secp256r1 (or NistP256 as it is shown in the policy editor). Additional ciphersuites and curves in each list will generate additional options in the client. A reboot of the system is required after changing the ciphersuite or elliptic curves configuration.



## Microsoft Windows 10 GP OS Administrative Guidance

### 6.3.6 Configuring key establishment schemes

Key lengths of keys used with certificates are configured in the certificate templates on the Certificate Authority used during enrollment and are not configured by the user or administrator. `

The IT administrator configures certificate templates for TLS client authentication as described in the following articles:

- Cryptography (for configuring the algorithm that the issued certificate's key pair will support): [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770477\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770477(v=ws.11))
- PowerShell commands for configuring the algorithm that the issued certificate's key pair will support: <https://docs.microsoft.com/en-us/powershell/module/tls/?view=win10-ps>

The administrator configures the correct algorithms for the given ciphersuites according to the following table:

Ciphersuites (per Security Target)	Selections in the certificate template
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246 TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246 TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 TLS_RSA_WITH_AES_128_GCM_SHA384 as defined in RFC 5288 TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289	Provider Category = Key Storage Provider  Algorithm Name = RSA



## Microsoft Windows 10 GP OS Administrative Guidance

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289	Provider Category = Key Storage Provider  Algorithm Name = ECDSA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	Provider Category = Key Storage Provider  Algorithm Name = ECDSA_P384

### 6.3.7 Managing signature algorithms with the Windows registry

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	All

The signature algorithm set that is acceptable to the client (offered in the signature\_algorithm extension during client hello) is configurable by editing the following registry key:

- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010003

Remove the signature algorithm that should not be used. No additional algorithms other than the default set may be specified.

### 6.3.8 Choosing TLS in a web browser

<b>Role</b>	Standard User
<b>Windows Editions</b>	All



Users may choose using TLS with HTTPS by using https in the URL typed into the browser.

## 6.4 Managing IPsec and VPN connections

<b>Role</b>	All
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

This section provides information on managing IPsec functionality and VPN connections on a device. The content in each subsection that follows addresses a specific aspect of IPsec or VPN configuration, most of which are exposed through the features of Windows Defender Firewall with Advanced Security. For an overview of all Windows Defender Firewall with Advanced Security features and a step-by-step deployment guide, see the following topic:

- Windows Defender Firewall with Advanced Security Deployment Guide: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security-deployment-guide>

### **Note:**

- File integrity self-testing of the Windows IPsec and VPN features occurs automatically. No configuration is necessary or possible.

### 6.4.1 Configuring IPsec firewall rules using Windows Defender Firewall with Advanced Security

The Windows Filtering Platform (WFP) is the IPsec Security Policy Database (SPD) for Windows. WFP starts automatically with Windows and must always be running to support IPsec scenarios. WFP features, including IPsec configuration, are exposed through the Windows Defender Firewall with Advanced Security features, which can be configured through the Windows Firewall with



## Microsoft Windows 10 GP OS Administrative Guidance

Advanced Security user interface, by Group Policy, with PowerShell, or with MDM. The following articles introduce how WFP operates and provide an overview of the IPsec configuration it enables:

- WFP Operation: <https://docs.microsoft.com/en-us/windows/win32/fwp/basic-operation>
- IPsec Configuration: <https://docs.microsoft.com/en-us/windows/win32/fwp/ipsec-configuration>

By establishing filter rules for inbound or outbound traffic, Windows Defender Firewall with Advanced Security can prevent traffic other than VPN traffic to and from a device. Common rules include Protect, Bypass, and Discard rules, which map to the following rule types in Windows Defender Firewall with Advanced Security:

- **Protect:** create a custom Outbound Rule, using the following parameters as a model:
  - Create a new outbound rule.
  - Choose protocol type: TCP.
  - Set the appropriate remote port, e.g. 8080.
  - Set the appropriate remote IP addresses the rule applies to, e.g. 192.168.5.102 and 192.168.4.0/24.
  - Select Allow the connection if it is secure.
  - Select Customize.
  - Select Allow the connection if it is authenticated and integrity-protected and click OK.
  - Select all domains.
  - Give the rule a name, e.g. ProtectRule2 and confirm the operation.
- **Bypass:** create a Connection Security Rule of the type Server to Server and choose to require authentication for inbound connections and request authentication for outbound connections.
- **Discard:** create a custom Inbound Rule with the action to block the connection.

Rules may be created using the Windows user interface, Group Policy, PowerShell, or MDM; see the subsections below for more information.

The following articles provide additional information on configuring common rules:



## Microsoft Windows 10 GP OS Administrative Guidance

- Create an Authentication Exemption List Rule: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-authentication-exemption-list-rule>
- Create an Inbound Program or Service Rule: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-inbound-program-or-service-rule>
- Create an Outbound Program or Service Rule: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-outbound-program-or-service-rule>

### 6.4.1.1 Configuring with the user interface

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard

To configure firewall rules described above using the user interface, follow these steps:

- Click **Start**.
- Type **Windows Defender Firewall with Advanced Security** to search for the app and open it.
- Click on the desired rule type from the left pane.
- From the **Actions** pane, choose **New Rule....**
- Follow the prompts and enter the required details.

### 6.4.1.2 Configuring with Group Policy

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter



An IT Administrator may define and deploy firewall rules like those described above via Group Policy. The policy objects are found under:

- **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security**

For more information on configuring Windows Firewall with Group Policy, see the following articles:

- Open the Group Policy Management Console to Windows Firewall with Advanced Security: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/open-the-group-policy-management-console-to-windows-firewall-with-advanced-security>
- Checklist: Creating Group Policy Objects: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/checklist-creating-group-policy-objects> (part of the Windows Defender Firewall with Advanced Security Deployment Guide)

#### 6.4.1.3 Configuring with PowerShell

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Windows Defender Firewall with Advanced Security may be administered using PowerShell cmdlets. This includes creating firewall rules. The following articles provide an overview and information on a selection of the cmdlets, including a description of the functionality and the syntax required for each:

- Windows Defender Firewall with Advanced Security Administration with Windows PowerShell: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security-administration-with-windows-powershell>
- Get-NetFirewallRule: <https://docs.microsoft.com/en-us/powershell/module/netsecurity/get-netfirewallrule?view=win10-ps>



## Microsoft Windows 10 GP OS Administrative Guidance

- New-NetFirewallRule: <https://docs.microsoft.com/en-us/powershell/module/netsecurity/new-netfirewallrule?view=win10-ps>
- Remove-NetFirewallRule: <https://docs.microsoft.com/en-us/powershell/module/netsecurity/remove-netfirewallrule?view=win10-ps>

There are additional PowerShell cmdlets available to manage firewall rules and related IPsec functionality. For a high-level overview of all PowerShell cmdlets related to network security, see the following article:

- NetSecurity: <https://docs.microsoft.com/en-us/powershell/module/netsecurity/?view=win10-ps>

### 6.4.1.4 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

Windows Defender Firewall with Advanced Security may be administered using MDM and the Firewall CSP. For detailed information, see the following topic:

- Firewall CSP: <https://docs.microsoft.com/en-us/windows/client-management/mdm/firewall-csp>

### 6.4.2 Configuring and using VPN connections and the VPN client

<b>Role</b>	
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

This section provides information on how to configure and use VPN connections and the RAS IPsec VPN client in Windows.

#### **Notes on VPN client configuration limitations:**



## Microsoft Windows 10 GP OS Administrative Guidance

- Windows supports Network Address Translation (NAT) traversal automatically as part of the IKEv1 and IKEv2 protocols. No configuration is needed or possible.
- Security association lifetime settings for IKEv2 may only be configured on the VPN gateway. No client configuration is needed or possible in the VPN client.
- For IKEv1 connections, Windows supports only main mode. It is not possible to configure IKEv1 to use aggressive mode.
- For IKEv1 connections, XAUTH is not supported.
- When using a pre-shared key, the secret value input into the client must match the secret value configured on the VPN server. The key must be at least 22 characters in length, but less than 256 characters. The key may be composed of any combination of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "\$", "%", "^", "&", "\*", "(", and ")".

### 6.4.2.1 Configuring VPN using VPN profiles and MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

An IT Administrator may use MDM to manage VPN profiles remotely on devices. VPN profiles support a variety of configuration options, including the following scenarios:

- Lockdown profiles, which force all network traffic to go through the VPN tunnel, other than the traffic necessary to establish the VPN connection (always-on VPN).
- Profiles that establish a VPN connection when a specified app is launched.
- Profiles that specify a connection type, e.g., IKEv1 (L2TP), IKEv1 (L2TP) with a pre-shared key, or IKEv2. Note: when using IKEv1 with a pre-shared key, the key is generated by the user or administrator.
- Profiles that specify an encryption algorithm, e.g. AES128 or AES256.

The following article describes the VPNv2 CSP, which may be used to implement any of the options listed above:

- VPNv2 CSP: <https://docs.microsoft.com/en-us/windows/client-management/mdm/vpnv2-csp>



## Microsoft Windows 10 GP OS Administrative Guidance

The following articles provide additional context by describing the different VPN profile options, including lockdown profiles, the VPN connection types supported (e.g., IKEv1, IKEv1 with a pre-shared key, or IKEv2), choosing an authentication method (e.g., PAP, CHAP, MSCHAPv2, or EAP), options for auto-triggering profiles, and additional parameters:

- VPN profile options: <https://docs.microsoft.com/en-us/windows/security/identity-protection/vpn/vpn-profile-options>
- VPN connection types: <https://docs.microsoft.com/en-us/windows/security/identity-protection/vpn/vpn-connection-type>
- VPN auto-triggered profile options: <https://docs.microsoft.com/en-us/windows/security/identity-protection/vpn/vpn-auto-trigger-profile>

Additionally, the following topic provides an example of how to create an Extensible Authentication Protocol (EAP) configuration XML for the VPN profile:

- EAP configuration: <https://docs.microsoft.com/en-us/windows/client-management/mdm/eap-configuration>

### 6.4.2.2 Configuring VPN using PowerShell

<b>Role</b>	Local Administrator, IT Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Windows PowerShell provides a variety of cmdlets to create and manage the VPN client and VPN connections. The following article provides an overview of all of the cmdlets related to the VPN client:

- VpnClient: <https://docs.microsoft.com/en-us/powershell/module/vpnclient/?view=win10-ps>

The Set-VpnConnection cmdlet may be used to specify the connection type (e.g., IKEv1 / L2TP, IKEv1 / L2TP with a pre-shared key, or IKEv2), the authentication method (e.g., PAP, CHAP, MSCHAPv2, or EAP), and many more parameters. Note: when using IKEv1 with a pre-shared key, the key is generated by the user or administrator. The following article provides more information on Set-VpnConnection:



## Microsoft Windows 10 GP OS Administrative Guidance

- Set-VpnConnection: <https://docs.microsoft.com/en-us/powershell/module/vpnclient/set-vpnconnection?view=win10-ps>

The Set-VpnConnectionIPsecConfiguration cmdlet may be used to specify additional IPsec parameters, including the encryption algorithm, e.g. AES128 or AES 256. The following article provides more information on Set-VpnConnectionIPsecConfiguration:

- Set-VpnConnectionIPsecConfiguration: <https://docs.microsoft.com/en-us/powershell/module/vpnclient/set-vpnconnectionipsecconfiguration?view=win10-ps>

## 6.4.2.3 Configuring a new VPN connection with the Windows UI

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise, Server Standard, Server Datacenter

The following steps outline how to create and configure a new connection in the Windows RAS IPsec VPN client, including choosing options for IKEv1, IKEv1 with a pre-shared key, and IKEv2.

- Open the **Settings** app
- Navigate to **Network & Internet** and choose **VPN**
- Choose **Add a VPN connection**
- From **VPN provider**, choose the option for **Windows (built in)**
- Enter the **Connection name** as a text string
- Enter the **Server name** or address as a DNS name or an IP address. Note that the Subject name of the server's certificate must match the DNS name or IP address entered.
- (Optional) to specify the connection type, choose one of the following:
  - For IKEv1, from **VPN type** choose **L2TP/IPsec with certificate**
  - For IKEv1 with a pre-shared key, from **VPN type** choose **L2TP/IPsec with pre-shared key** and enter the text of the key
  - For IKEv2, from **VPN type** choose the **IKEv2** option and choose **Certificate** as the type of sign-in info (see the additional note below if using machine certificates)



## Microsoft Windows 10 GP OS Administrative Guidance

- Choose the authentication method from **Type of sign-in info**
- Configure the user credentials as appropriate
- **Save** the connection
- **Note if using machine certificates:** To configure the VPN connection to use machine certificates, you must adjust the properties via the Adapter Properties feature.
  - Open **Network Connections** from the Control Panel (or, choose **Change adapter options** from the VPN panel in Settings).
  - Right-click on the VPN connection and select **Properties**.
  - Select the **Security** tab.
  - Select the **Use machine certificates** option.

## 6.4.2.4 Connecting to a VPN gateway with the Windows UI

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise, Server Standard, Server Datacenter

The following steps outline how to connect to a VPN gateway once a VPN connection has been configured.

- Open the **Settings** app
- Navigate to **Network & Internet** and choose **VPN**
- Select the desired VPN connection and choose **Connect**
- If the device should always attempt to connect to this VPN connection, choose the **Connect automatically** checkbox

## 6.4.2.5 VPN client SA lifetime

SA lifetime settings for tunnel mode using the RAS IPsec VPN interface for IKEv1 and IKEv2 are configured on the VPN gateway. The following are the default values used for lifetimes by the RAS IPsec VPN Client:

- Main Mode



## Microsoft Windows 10 GP OS Administrative Guidance

- Lifetime in Seconds: 10800
- Quick Mode
  - Lifetime in Seconds: 3600
  - Lifetime in Packets: 2147483647
  - Lifetime in Kilobytes: 250000
  - Idle Duration in Seconds: 300

If a connection is broken due to network interruption, then the established SA remains in use until the SA lifetime limits are reached.

### 6.4.3 Configuring security association (SA) parameters

Windows supports a variety of parameters to configure security associations (SAs) between devices.

#### 6.4.3.1 Configuring IPsec in transport mode

<b>Role</b>	Local Administrator, IT Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Windows supports transport mode security associations (SAs) via the IKEv2 protocol. IKEv2 connections are configured using Windows PowerShell cmdlets. The following article describes how to secure IPsec connections using IKEv2:

- Securing end-to-end IPsec connections by using IKEv2: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/securing-end-to-end-ipsec-connections-by-using-ikev2>

For additional information about IPsec transport mode scenarios in Windows, see the following article:

- IPsec Configuration – Transport Mode: <https://docs.microsoft.com/en-us/windows/win32/fwp/regular-transport-mode>
- IPsec Configuration - Tunnel Mode: <https://docs.microsoft.com/en-us/windows/win32/fwp/tunnel-mode>



## Microsoft Windows 10 GP OS Administrative Guidance

### 6.4.3.2 Configuring IKEv1 security association lifetime in transport mode using PowerShell or Group Policy

<b>Role</b>	Local Administrator, IT Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Security association (SA) lifetime for IKEv1 connections may be configured locally. (For IKEv2 connections, SA lifetimes may be configured on the VPN gateway only; configuring the VPN gateway is out of the scope of this administrative guide.) Windows PowerShell cmdlets are the preferred solution to configure IKEv1 SA lifetime, among other parameters, for both main mode (phase 1) and quick mode (phase 2). The following articles provide information for each scenario:

PowerShell cmdlets:

- New-NetIPsecMainModeCryptoSet – see the parameters MaxMinutes and MaxSessions for SA lifetime control:  
<https://docs.microsoft.com/en-us/powershell/module/netsecurity/new-netipsecmainmodecryptoset?view=win10-ps>

PowerShell configuration of quick mode:

- New-NetIPsecQuickModeCryptoProposal – see the parameters MaxKiloBytes and MaxMinutes for SA lifetime control:  
<https://docs.microsoft.com/en-us/powershell/module/netsecurity/new-netipsecquickmodecryptoproposal?view=win10-ps>

### 6.4.3.3 Configuring authentication signature algorithms

<b>Role</b>	Local Administrator, IT Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Windows supports the following signature algorithms for IPsec authentication with certificates:

- RSA



## Microsoft Windows 10 GP OS Administrative Guidance

- ECDSA P256
- ECDSA P384

The New-NetIpssecAuthProposal PowerShell cmdlet is used to configure authentication techniques to be used and the signature algorithms to use with certificate authentication. The following topic provides more information:

- New-NetIpssecAuthProposal: <https://docs.microsoft.com/en-us/powershell/module/netsecurity/new-netipsecauthproposal?view=win10-ps>

The SubjectName and SubjectNameType options combined with the ValidationCriteria option for the New-NetIpssecAuthProposal cmdlet are used to configure how the name of the remote certificate will be verified. See topic above for information on what values are acceptable for the SubjectNameType parameter. In order to support an IP address in the remote entity's certificate, the remote entity's certificate subject name may be a Common Name (CN) with the IP address as the value of the Common Name. In addition, the RemoteAddress and SubjectName options for the New-NetIpssecAuthProposal cmdlet must be set to the IP address in the certificate.

### 6.4.3.4 Configuring certificate validation and revocation checks

<b>Role</b>	Local Administrator, IT Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Windows performs certificate validation by default when using IPsec with certificates. No configuration is necessary to enable certificate validation. To configure Windows to require certificate revocation checking, use the Set-NetFirewallSetting PowerShell cmdlet. The same PowerShell cmdlet may be used to configure a Group Policy object, which can then be distributed via Group Policy. The following topic provides more information:

- Set-NetFirewallSetting – use the RequireCrlCheck value for the CertValidationLevel parameter: <https://docs.microsoft.com/en-us/powershell/module/netsecurity/set-netfirewallsetting?view=win10-ps>



## Microsoft Windows 10 GP OS Administrative Guidance

Note that extensions in a certificate specify the mechanism(s) to perform revocation checking for the particular certificate, either CRL or OCSP; the RequireCrlCheck setting applies to whichever revocation mechanism(s) are specified in certificates. Windows will automatically use a protected communication path with the entity providing the revocation information when such a communication path is configured in the certificate being validated. For example, if the CRL distribution point is a HTTPS URL in the extension in the certificate or if the OCSP server uses a HTTPS URL in the extension in the certificate then Windows will use HTTPS for the communication path with the CRL distribution point or the OCSP server.

### 6.4.3.5 Using pre-shared keys

<b>Role</b>	Local Administrator, IT Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Windows supports the use of pre-shared keys for IKEv1 / L2TP connections. The secret value for the pre-shared key must be a text-based value manually entered in the input field for a pre-shared key. The secret value input into the client must match the secret value configured on the VPN server. The key must be at least 22 characters in length, but less than 256 characters. The key may be composed of any combination of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "\$", "%", "^", "&", "\*", "(", and ")".

## 6.5 Managing network connections

This section collects configuration information for networking, including both wired Local Area Network (LAN) connections and Wireless Local Area Network (WLAN or Wi-Fi) connections.

### 6.5.1 Enabling or disabling network connections with the Windows UI

<b>Role</b>	Standard User
-------------	---------------



## Microsoft Windows 10 GP OS Administrative Guidance

<b>Windows Editions</b>	Home, Pro, Enterprise
-------------------------	-----------------------

The following article provides details on enabling and disabling wired and wireless network connections with the Windows user interface:

- Enable or disable a network connection: [https://technet.microsoft.com/en-us/library/cc771762\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc771762(v=ws.10).aspx)

### 6.5.2 Enabling or disabling network connections with PowerShell

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	All

Network connections may also be enabled and disabled using PowerShell. The following articles provide information on how to enable and disable network adapters with PowerShell:

- Disable-NetAdapter: <https://docs.microsoft.com/en-us/powershell/module/netadapter/disable-netadapter?view=win10-ps>
- Enable-NetAdapter: <https://docs.microsoft.com/en-us/powershell/module/netadapter/enable-netadapter?view=win10-ps>

### 6.5.3 Configuring Wi-Fi access with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

The availability of Wi-Fi and several Wi-Fi settings may be configured by the IT Administrator using MDM. See the MDM solution



## Microsoft Windows 10 GP OS Administrative Guidance

documentation for detailed configuration actions. The following articles provide information on the two relevant CSPs for managing Wi-Fi with MDM:

- <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-wifi>
- <https://docs.microsoft.com/en-us/windows/client-management/mdm/wifi-csp>

### 6.5.4 Configuring Wi-Fi access with the Windows user interface

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise

The wireless network adapter is enabled or disabled via the Windows Settings app.

- Open **Settings**
- Navigate to **Network & Internet** > **Status** > **Change adapter options**
- In the **Network Connections** window, select the Wi-Fi adapter and click the **Disable this network device** or **Enable this network device** button.

The articles below provide additional information on configuring Wi-Fi and troubleshooting:

- <https://support.microsoft.com/en-us/help/17137/windows-setting-up-wireless-network>
- <https://support.microsoft.com/en-us/help/4000432/windows-10-fix-wi-fi-problems>

### 6.5.5 Configuring allowed Wi-Fi networks with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise



## Microsoft Windows 10 GP OS Administrative Guidance

An IT Administrator may specify the set of wireless networks (SSIDs) that a client is allowed to connect to using MDM. See the MDM solution documentation for detailed configuration actions. The following article provides information on the relevant CSP for configuring allowed SSIDs.

- <https://docs.microsoft.com/en-us/windows/client-management/mdm/wifi-csp>

### 6.5.6 Configuring allowed Wi-Fi networks with Group Policy

<b>Role</b>	IT Administrator, Local Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Group policy can be used to specify the wireless networks (SSIDs) that a user may connect to.

- Configure Network Permissions and Connection Preferences: <https://msdn.microsoft.com/en-us/library/dd759204.aspx>

### 6.5.7 Selecting a secure Wi-Fi connection with the Windows UI

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise

The following steps outline how to select and connect to an available Wi-Fi network using a higher level of security:

- Open the **Start** button
- Navigate to **Settings > Network & Internet > Wi-Fi > Show available networks**
- Choose the network you want to connect to, select **Connect**, type the network password if necessary, then select **Next**



If the Wi-Fi connection is unintentionally broken, Windows will automatically attempt to reconnect to the same connection when it becomes available again. No action is required by the user.

### 6.5.8 Configuring a Wi-Fi connection profile with the Windows UI

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise

The following steps provide information on how to manually configure a WLAN connection profile (e.g. EAP-TLS using WPA2-Enterprise) using the Windows user interface.

 **Note:** Configuration options may be different depending on the specific selections for your environment.

- Open the **Control Panel**
- Navigate to **Network and Sharing Center**
- Select **Set up a new connection or network**
- Select **Manually connect to a wireless network** to create a new WLAN profile
- In the **Network name** box, enter the name of the SSID to connect to
- From the **Security type** list, choose the security type (e.g. WPA2 Enterprise)
- Select **Next** and then **Change connection settings** to open the **<SSID name> Wireless Network Properties** window
- Select the **Security** tab
- Choose the authentication method from the **Choose a network authentication method** list (e.g. for EAP-TLS certificate-based authentication choose "Microsoft: Smart card or other certificate")
- Select **Advanced Settings**, which will bring up a window with the **802.1X settings** tab
- Check the **Specify authentication mode** checkbox and then select the type of authentication certificate that has been configured (e.g. "User authentication" for a client authentication certificate)
- In the same window, configure the PMK caching if desired



## Microsoft Windows 10 GP OS Administrative Guidance

- In the same window, configure pre-authentication for the WLAN network if desired
- Select **OK** to return to the <SSID name> **Wireless Network Properties** window
- On the **Security** tab click **Settings** to open the **Smart Card or other Certificate Properties** window
- Check **Use a certificate on this computer** and click the **Advanced** button to open the **Configure Certificate Selection** window
- Check the **Certificate Issuer** checkbox and then in the **Select one or multiple certificate issuers to be used for the certificate** list, check the Certificate Authority that issued the authentication certificate(s) configured on the client
- Click **OK** to return to the **Smart Card or other Certificate Properties** window
- Check the **Verify the server's identity by validating the certificate** if desired
- Check the **Connect to these servers...** checkbox if desired and enter the FQDN of acceptable WLAN server authentication server certificates in the textbox
- Check the Certificate Authority corresponding to the certificate issuer for the server certificate configured on the WLAN authentication server and then click **OK**
- Click **Close** to complete configuration for the WLAN connection profile

## 6.6 Managing personal hotspots

This section provides information on allowing or disallowing personal hotspots (internet sharing) on a device.

 **Note:** The guidance in this section applies to all forms of authentication to the personal hotspot, including pre-shared keys.

### 6.6.1 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

Sharing a personal hotspot may be enabled/disabled may be managed by the IT Administrator using MDM. See the MDM solution



## Microsoft Windows 10 GP OS Administrative Guidance

documentation for detailed management actions. The following article describes the CSP that enables MDM to affect the policy for personal hotspots:

- Wi-Fi CSP: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-wifi#wifi-allowinternetsharing>

### 6.6.2 Configuring with group policy

<b>Role</b>	IT Administrator, Local Administrator,
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Administrators can use group policy to enable or disable the use of hotspot sharing. The policy objects are found under:

- **Computer configuration > Administrative templates > Network > Network Connections**

The two group policy objects are:

- Prohibit use of Internet Connection Sharing on your DNS Domain network
- Prohibit installation and configuration of Network Bridge on your DNS Domain network

### 6.6.3 Configuring with the Windows user interface

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise

Standard users can enable or disable hotspot sharing via Windows Settings:

- Open the **Start** menu
- Navigate to **Settings > Network & Internet > Mobile hotspot**



- Select a connection from the dropdown, **Share my internet connection from**
- If desired, tap the **Edit** button to configure the SSID name and password
- Turn **Mobile hotspot** to **On**

## 6.7 Managing Bluetooth

This section provides various configuration instructions for managing Bluetooth.

### **Notes:**

- No additional configuration is necessary to ensure the Bluetooth services provided before login are limited.
- No additional configuration is necessary to ensure Bluetooth pairing uses a protected communication channel.

### 6.7.1 Configuring Bluetooth adapters with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

The Bluetooth radio may be configured by the IT Administrator using MDM. See the MDM solution documentation for detailed configuration actions. The following article describes the CSP that enables MDM to affect the policy for Bluetooth:

- Policy CSP, Connectivity function: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-connectivity#connectivity-allowbluetooth>.

### 6.7.2 Configuring Bluetooth properties with MDM

<b>Role</b>	IT Administrator
-------------	------------------



<b>Windows Editions</b>	Pro, Enterprise
-------------------------	-----------------

IT Administrators may configure multiple Bluetooth properties via MDM. These include enabling and disabling discoverable mode (for BR/EDR), changing the Bluetooth device name, enabling or disabling advertising mode (for LE), and configuring the available profiles. The following article provides information on the Bluetooth node of the Policy CSP, which is used to manage Bluetooth properties:

- Policy CSP – Bluetooth: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-bluetooth>

### 6.7.3 Enabling or disabling Bluetooth adapters via Device Manager

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	Home, Pro, Enterprise

A user or administrator may enable or disable the Bluetooth adapter with the Windows Device Manager. The steps to do so are:

- Open **Device Manager**
- Locate the **Bluetooth** node and expand it
- Right-click on the appropriate Bluetooth adapter and choose **Properties**
- Select the **Driver** tab
- Choose **Disable Device** to disable it or **Enable Device** to enable it

### 6.7.4 Enabling or disabling Bluetooth adapters with PowerShell

<b>Role</b>	Standard User, Local Administrator
-------------	------------------------------------



<b>Windows Editions</b>	All
-------------------------	-----

A user or administrator may enable or disable the Bluetooth adapter with a PowerShell script that leverages Windows Device Manager extensibility. The following article provides the details on the script:

- Disable Bluetooth in Windows 10: <https://blogs.technet.microsoft.com/letsdothis/2017/06/20/disable-bluetooth-in-windows-10-updated/>

### 6.7.5 Pairing Bluetooth devices with the Windows UI

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	Home, Pro, Enterprise, Server Standard

The Windows user interface provides a straightforward way for users to pair Bluetooth devices. For complete information, including the specific authorization screens, see the following article:

- Connect a Bluetooth device: <https://support.microsoft.com/en-au/help/15290/windows-connect-bluetooth-device>

## 6.8 Managing passwords and password policy

The following sections provide multiple options for managing password policies.

### 6.8.1 Configuring with MDM

<b>Role</b>	IT Administrator
-------------	------------------



<b>Windows Editions</b>	Pro, Enterprise
-------------------------	-----------------

Password policy may be configured using MDM. The DeviceLock and CredentialsUI policies, part of the larger Policy CSP, provide a variety of management functions for password policy. Note that some DeviceLock functions may not be available on Windows Home. The documentation for each function notes which editions the function may be used with. The following articles provide an overview of DeviceLock and a listing of all functions available:

- Policy CSP – overview, including a list of all DeviceLock policies: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider>
- Policy CSP – DeviceLock policy functions: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock>
- Policy CSP – CredentialsUI: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-credentialsui>

The following sample of DeviceLock policy functions address common needs of IT administrators. The article links provide detailed information on the policy function and how to implement it.

- Requiring a password: Use the policy **DeviceLock/DevicePasswordEnabled**. For more information, see: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock#devicelock-devicepasswordenabled>.
- Disabling the Guest account: Use the policy **LocalPoliciesSecurityOptions/Accounts\_EnableGuestAccountStatus**. For more information, see: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-localpoliciessecurityoptions#localpoliciessecurityoptions-accounts-enableguestaccountstatus>.
- Specifying password length: Use the policy **DeviceLock/MinDevicePasswordLength**. For more information, see: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock#devicelock-mindevicepasswordlength>.
- Specifying password complexity: Use the policy **DeviceLock/MinDevicePasswordComplexCharacters**. For more information, see: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock#devicelock-mindevicepasswordcomplexcharacters>.



## Microsoft Windows 10 GP OS Administrative Guidance

- Specifying password expiration: Use the policy **DeviceLock/DevicePasswordExpiration**. For more information, see: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock#devicelock-devicepasswordexpiration>
- Disabling the password reveal button: Use the policy **CredentialsUI/DisablePasswordReveal**. For more information, see: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-credentialsui#credentialsui-disablepasswordreveal>

### 6.8.2 Configuring with group policy

<b>Role</b>	IT Administrator, Local Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Password policy may be configured using group policy. The Password Policy set, part of the larger Account Policies, provide a variety of management functions for password policy. The following article provides an overview:

- Password Policy: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy>

The following sample of Password Policy functions address common needs of IT administrators. The article links provide detailed information on the policy function and how to implement it.

- Disabling the Guest account: Use the setting **Accounts: Guest account status** under **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**. For more information, see: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-guest-account-status>.
- Specifying password length: Use the setting **Minimum password length** under **Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy**. For more information, see: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/minimum-password-length>.
- Specifying password complexity: Use the setting **Passwords must meet complexity requirements** under **Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy**. For more information, see:



<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements>

- Specifying the maximum number of authentication failures: Use the setting **Account lockout threshold** under **Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy** to set the maximum number of failures. For more information, see: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold>.
- Specifying the duration within which to enforce the maximum number of authentication failures: Use the setting **Account lockout duration** under **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**. For more information, see: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-duration>.
- Specifying password expiration: Use the setting **Maximum password age** under **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**. For more information, see: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/maximum-password-age>.
- Disabling the password reveal button: Use the setting **DisablePasswordReveal** under **Computer Configuration\Administrative Templates\Windows Components\Credential User Interface**.

### 6.8.3 Configuring with net.exe accounts utility

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	All

The net.exe accounts utility may be used to manage some aspects of password and account lockout policy. The management functions available via net accounts include:

- Forcing user logoff after a time interval
- Minimum and maximum password age (days)
- Minimum password length



## Microsoft Windows 10 GP OS Administrative Guidance

- Length of password history maintained
- Lockout threshold
- Lockout duration (minutes)
- Lockout observation window (minutes)

The following article provides an overview of net accounts and how to use it:

- Net Accounts: <http://technet.microsoft.com/en-us/library/bb490698.aspx>

In addition to the parameters given in the referenced article the following are also valid options:

- **/lockoutthreshold:number:** Sets the number of times a bad password may be entered until the account is locked out. If set to 0 then the account is never locked out.
- **/lockoutwindow:minutes:** Sets the number of minutes of the lockout window.
- **/lockoutduration:minutes:** Sets the number of minutes the account will be locked out for.

## 6.9 Managing smart card logon

<b>Role</b>	IT Administrator, Local Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Smartcard logon is supported on Windows domain-joined devices. IT administrators must enable an account for smartcard logon and issue a smartcard to a user. For more information about how smart card authentication works in Windows and how to enable it, see the following article and its sub-articles:

- How Smart Card Sign-in Works in Windows: <https://docs.microsoft.com/en-us/windows/security/identity-protection/smart-cards/smart-card-how-smart-card-sign-in-works-in-windows>



## Microsoft Windows 10 GP OS Administrative Guidance

For more information on how an IT administrator may configure Windows to require a smart card for interactive login, see the following article:

- <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-login-require-smart-card>

## 6.10 Managing Windows Hello

### 6.10.1 Configuring biometric authentication with the Windows UI

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise

To enable Windows Hello and add authentication mechanisms other than password, follow these steps.

- Login to the user account
- Navigate to **Settings** > **Accounts** > **Sign-in options**
- Review the Windows Hello options and select either **Fingerprint** or **Face Recognition**
- Follow the instructions in the Windows Hello setup wizard
- Sign out

### 6.10.2 Configuring Windows Hello for Business with group policy or MDM

<b>Role</b>	IT Administrator, Local Administrator
<b>Windows Editions</b>	Pro, Enterprise



Windows Hello for Business is the recommended solution to replace passwords with strong two-factor authentication on Windows devices joined to a domain or managed by MDM. Windows Hello for Business offers a variety of policy options that can be implemented by either group policy or MDM. The articles below provide an overview, planning guide, and implementation details:

- Windows Hello for Business: <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-identity-verification>
- Manage Windows Hello for Business in your organization (including group policy and MDM policy settings): <https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-manage-in-organization>

### 6.10.3 Configuring PIN authentication with the Windows UI

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise

To enable a PIN in place of passwords, follow these steps:

- Login to the user account
- Navigate to **Settings > Accounts > Sign-in options**
- Under the **PIN** heading tap the **Add** button
- Choose a new PIN value in the **Set a PIN** window. This requires entering a username and password to confirm the operation
- Sign out



## 6.11 Managing screen lock and session timeout

### 6.11.1 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

The Policy CSP provides IT Administrators with multiple options for configuring screen lock and session timeout. The documentation for each policy notes which Windows editions the policy may be applied to. The following article provide an overview of the Policy CSP:

- Policy CSP: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-configuration-service-provider>

The DeviceLock node of the Policy CSP provides many policies to control device locking scenarios, including enabling screen lock, setting the lock timeout period, and more. See the following article provides more information on each DeviceLock policy:

- Policy CSP – DeviceLock: Policy CSP – overview, including a list of all DeviceLock policies: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock>

The AboveLock node of the Policy CSP provides policies to control the scope of notifications displayed above the lock screen when a device is locked. The following article provides more information on each AboveLock policy:

- Policy CSP – AboveLock: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-abovelock>

### 6.11.2 Configuring with group policy

<b>Role</b>	IT Administrator, Local Administrator
-------------	---------------------------------------



## Microsoft Windows 10 GP OS Administrative Guidance

<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter
-------------------------	---

Screen lock and session timeout can both be configured by group policy. The relevant policy is:

- **Interactive logon: Machine inactivity limit** under **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**. For more information, see <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-machine-inactivity-limit>.

### 6.11.3 Configuring with the Windows registry

<b>Role</b>	Local Administrator, Standard User
<b>Windows Editions</b>	All

The following articles provide information on registry settings which may be used to configure screen lock:

- ScreenSaveActive: <https://technet.microsoft.com/en-us/library/cc978620.aspx>
- ScreenSaverIsSecure: <https://technet.microsoft.com/en-us/library/cc959646.aspx>
- ScreenSaveTimeout: <https://technet.microsoft.com/en-us/library/cc978621.aspx>

### 6.11.4 Transitioning to the locked state with the Windows user interface

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise

The user has two options to initiate a screen lock manually:



## Microsoft Windows 10 GP OS Administrative Guidance

- Click on the **Start** button > click on the user picture (upper left in Start Menu) > click **Lock**.  
- or -
- Type the Windows logo key + L

## 6.12 Managing the logon banner

### 6.12.1 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

The logon banner message to users may be configured by the IT administrator using MDM. See the MDM solution documentation for detailed configuration actions. . The following article describes the CSP to manage the logon banner:

- Policy CSP – LocalPoliciesSecurityOptions: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-localpoliciessecurityoptions#localpoliciessecurityoptions-interactive-logon-display-user-information-when-the-session-is-locked>.

### 6.12.2 Configuring with group policy

<b>Role</b>	IT Administrator, Local Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

The following articles describe how to configure a message to users attempting to logon with the Group Policy Editor or Local Security Policy Editor:



## Microsoft Windows 10 GP OS Administrative Guidance

- Interactive logon: Message title for users attempting to log on:  
<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-message-title-for-users-attempting-to-log-on>
- Interactive logon: Message text for users attempting to log on:  
<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>

### 6.12.3 Configuring with the Windows registry

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	All

The logon banner message may also be configured by modifying the following Windows registry key values, which affect the user notification that displays at logon. Note that a reboot of the machine is required after modifying the keys to see the updated logon banner. The two registry keys are:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\legalnoticecaption – affects the string that displays as the caption of the legal notice dialog box
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\legalnoticetext – affects the string that displays as the message of the legal notice dialog box

## 6.13 Managing USB

### 6.13.1 Configuring via Device Manager

<b>Role</b>	Local Administrator
-------------	---------------------



## Microsoft Windows 10 GP OS Administrative Guidance

<b>Windows Editions</b>	Home, Pro, Enterprise, Server Standard
-------------------------	--

An administrator or user may enable or disable USB ports using the Windows Device Manager. To do so, follow these steps:

- Open the **Device Manager**
- Find the **Universal Serial Bus controllers** node and expand it
- Right-click on the **USB Root Hub** child node and select the **Properties** menu item to open the **USB Root Hub Properties** window
- Select the **Driver** tab and click the **Enable** or **Disable** button

### 6.13.2 Configuring with PowerShell

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	All

USB controllers may be enabled or disabled with PowerShell. The following articles describe the PowerShell cmdlets that may be used to disable USB controllers:

- Get-PnpDevice: <https://docs.microsoft.com/en-us/powershell/module/pnpdevice/get-pnpdevice?view=win10-ps>
- Disable-PnpDevice: <https://docs.microsoft.com/en-us/powershell/module/pnpdevice/disable-pnpdevice?view=win10-ps>
- Enable-PnpDevice: <https://docs.microsoft.com/en-us/powershell/module/pnpdevice/enable-pnpdevice?view=win10-ps>

### 6.13.3 Configuring with the Windows registry

<b>Role</b>	Local Administrator
-------------	---------------------



<b>Windows Editions</b>	All
-------------------------	-----

The Windows registry may also be used to manage USB. Specifically, to disable the use of USB storage devices:

- Find the registry key, HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\UsbStor
- Change the Start REG\_DWORD value to 4. (The default is 3.)
- Restart the machine.


For more information on the CurrentControlSet\Services registry tree, see this article:

- HKLM\SYSTEM\CurrentControlSet\Services Registry Tree: <https://docs.microsoft.com/en-us/windows-hardware/drivers/install/hklm-system-currentcontrolset-services-registry-tree>

## 6.14 Managing updates

The following article provides an overview of Windows Update and a matching set of FAQs:

- Windows Update FAQ: <https://support.microsoft.com/en-us/help/12373/windows-update-faq>

 **Note:** Windows Update may be configured to use enterprise Windows Server Update Services (WSUS) rather the default Microsoft Update. Configuring WSUS is outside the scope of this document.

### 6.14.1 Configuring using MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise



## Microsoft Windows 10 GP OS Administrative Guidance

The IT administrator may configure Automatic Updates or Windows Server Update Services (WSUS) using the MDM. See the MDM solution documentation for detailed actions. The following article describes the CSP policy for managing updates:

- Policy CSP – Update: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-update#update-policies>

### 6.14.2 Configuring using group policy

<b>Role</b>	IT Administrator, Local Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

The following article provides details on configuring updates using domain group policy:

- Configure Group Policy Settings for Automatic Updates: <https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-configure-group-policy-settings-for-automatic-updates>

### 6.14.3 Configuring using the Server Configuration tool

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	Server Standard Core, Server Datacenter Core

The Server Configuration tool (sconfig.cmd) is available to configure Windows Update and other features on Windows Server installations. The following topic describes how to use sconfig to configure Windows Server, including the Windows Update settings:

- Configure a Server Core installation of Windows Server 2016 or Windows Server, version 1709, with Sconfig.cmd: <https://docs.microsoft.com/en-us/windows-server/get-started/sconfig-on-ws2016#windows-update-settings>



#### 6.14.4 Checking for OS updates using the Windows UI

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise, Server Standard

To check for Windows updates, follow these steps:

- Open **Settings**
- Navigate to **Update & security**
- Click the Check for updates button.

#### 6.14.5 Querying for Windows version and hardware information

<b>Role</b>	Standard User, Local Administrator, IT Administrator
<b>Windows Editions</b>	Home, Pro, Enterprise, Server Standard

The Windows user interface and PowerShell may be used to query for Windows version information. The following article provides details on how to do this via System Properties, System Info, the Command Prompt, and PowerShell:

- What version of Windows am I running? <https://docs.microsoft.com/en-us/windows/client-management/windows-version-search>

To query for hardware information and detailed Windows version information, leverage the systeminfo command. The following article provides details on systeminfo:

- Systeminfo: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/systeminfo>

IT administrators may also query for Windows version and hardware information with MDM. The DevDetail CSP returns many device-specific parameters to the device management server. The following topic provides detailed information on the DevDetail CSP:



## Microsoft Windows 10 GP OS Administrative Guidance

- DevDetail CSP: <https://docs.microsoft.com/en-us/windows/client-management/mdm/devdetail-csp>

### 6.14.6 Installing Windows updates via the command line

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	All

Windows update packages may be installed manually via the command line interface on Windows 10 and Windows Server editions. The Windows Update Standalone Installer (Wusa.exe) provides features that enable manual installation. For details on how to use Wusa.exe to, see the following articles:

- Patch a Server Core installation: <https://docs.microsoft.com/en-us/windows-server/administration/server-core/server-core-servicing> (for Server Core)
- Windows Update Standalone Installer in Windows: <https://support.microsoft.com/en-us/help/934307/description-of-the-windows-update-standalone-installer-in-windows> (for all editions)

### 6.14.7 Checking for Windows Store application updates

<b>Role</b>	Standard User
<b>Windows Editions</b>	Home, Pro, Enterprise

The following article describes how to check for updates to applications installed from the Windows Store:

- Check for updates for apps and games from Windows Store: <https://support.microsoft.com/en-us/help/4026259/microsoft-store-check-updates-for-apps-and-games>



### 6.14.8 Querying for installed application version information

<b>Role</b>	Standard User, Local Administrator, IT Administrator
<b>Windows Editions</b>	Home, Pro, Enterprise, Server Standard

The PowerShell Get-AppxPackage cmdlet may be used to gather detailed information, including version, on all app packages installed for one or more users on a device. The following article provides detailed information on the Get-AppxPackage cmdlet:

- Get-AppxPackage: <https://docs.microsoft.com/en-us/powershell/module/appx/get-appxpackage?view=win10-ps>

IT administrators may also leverage MDM to query for installed application version information. The following article provides more information on the EnterpriseModernAppManagement CSP, which enables this:

- EnterpriseModernAppManagement CSP: <https://docs.microsoft.com/en-us/windows/client-management/mdm/enterprisemodernappmanagement-csp>

## 6.15 Managing diagnostic data

Windows offers granular control over the diagnostic data that is collected and shared with Microsoft. This section provides multiple solutions to control diagnostic data. See the following topic for an overview of what diagnostic data is, how it benefits the ongoing development of Windows, and how customers can control it:

- Configure Windows diagnostic data in your organization: <https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization>

### 6.15.1 Configuring with group policy

<b>Role</b>	IT Administrator, Local Administrator
-------------	---------------------------------------



## Microsoft Windows 10 GP OS Administrative Guidance

<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter
-------------------------	---

The diagnostic data level and diagnostic components may be managed using group policy. The following topic outlines the different data level settings available and how to implement them via group policy:

- Configure Windows diagnostic data in your organization, Enterprise management section: <https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization#enterprise-management>

### 6.15.2 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

The diagnostic data level and diagnostic components may be managed using MDM. The following topic outlines the different data level settings available and a high-level guide to implementing them via MDM:

- Configure Windows diagnostic data in your organization, Enterprise management section: <https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization#enterprise-management>

The System/AllowTelemetry policy within the Policy CSP is the solution for managing diagnostic data with MDM. The following topic provides detailed information on the Policy CSP and, specifically, the System/AllowTelemetry policy:

- Policy CSP – System, System/AllowTelemetry section: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-system#system-allowtelemetry>



### 6.15.3 Configuring with the Windows UI

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	Home

The diagnostic data level may be managed via the Settings app in the Windows UI.

- Open the **Settings** app
- Navigate to the **Privacy** category
- Choose **Diagnostics & feedback**
- Choose the desired **Diagnostic data** level

## 6.16 Managing the firewall

### 6.16.1 Configuring with PowerShell

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	All

The following article describes how the Windows Firewall is managed using PowerShell cmdlets:

- Network Security Cmdlets in Windows PowerShell: <https://docs.microsoft.com/en-us/powershell/module/netsecurity/?view=win10-ps>




## 6.17 Managing domains

The following article provides an overview of how to join a client computer to an Active Directory domain:

- How to Join Your Computer to a Domain: <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/join-a-computer-to-a-domain>

The name of the domain that is indicated for the Domain entry in step (2) should be provided by your IT administrator.

 **Note:** Choosing a domain is equivalent to enrolling with a MDM.

### 6.17.1 Configuring with PowerShell

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	All

The following article describes how to join a computer to a domain using PowerShell:

- Add-Computer: <https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/add-computer?view=powershell-5.1>

## 6.18 Managing date and time

### 6.18.1 Configuring with PowerShell

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	All



## Microsoft Windows 10 GP OS Administrative Guidance

An administrator or user may set the date and time on a client using the Set-Date PowerShell cmdlet that is documented here:

- Using the Set-Date Cmdlet: <https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/set-date?view=powershell-6>

### 6.18.2 Configuring with Windows Time Service Tools

<b>Role</b>	All
<b>Windows Editions</b>	All

A dedicated set of tools are available to administrators to manage the Windows Time Service and related settings, including configuring the name and address of the time server. The following article describes the W32tm command, used to synchronize with a time server:

- Windows Time Service Tools and Settings: <https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/windows-time-service-tools-and-settings>

### 6.18.3 Configuring with the Windows user interface

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	Home, Pro, Enterprise

The Windows Settings app may be used to configure the date, time, and time zone.

- Open the **Settings** app.
- Choose **Time & language**.



- Choose **Date & time**.
- Choose the desired options.

## 6.19 Managing remote administration

The following articles provide overview information remote desktop services and clients, including how to establish a trusted remote session:

- Remote Desktop Services Overview: <https://technet.microsoft.com/en-us/library/hh831447.aspx>
- Microsoft Remote Desktop Clients: [https://technet.microsoft.com/en-us/library/dn473009\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn473009(v=ws.11).aspx)

Securing remote sessions (RDP session security) is controlled by the RDP host in most cases. The following link provides information on how to require TLS for RDP sessions:

- Configure Server Authentication and Encryption Levels: <https://technet.microsoft.com/en-us/library/cc770833.aspx>

Note that TLS 1.2 will be negotiated using the above settings.

The following link provides information on configuring Session Time Limits for remote connections:

- Session Time Limits: <https://technet.microsoft.com/en-us/library/cc753112.aspx>

### 6.19.1 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

Remote administration may be managed remotely by the IT Administrator using MDM. The following article describes the correct function in the Policy CSP to use:



## Microsoft Windows 10 GP OS Administrative Guidance

- Policy CSP – RemoteDesktopServices: <https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-remotedesktopservices>

### 6.19.2 Configuring with group policy

<b>Role</b>	IT Administrator, Local Administrator
<b>Windows Editions</b>	Pro, Enterprise, Server Standard, Server Datacenter

Windows may be managed remotely by the IT Administrator using domain group policy. The following link describes Managing Group Policy:

- Managing Group Policy: <https://technet.microsoft.com/en-us/library/cc978280.aspx>

### 6.19.3 Configuring with PowerShell

<b>Role</b>	Standard User, Local Administrator
<b>Windows Editions</b>	All

Windows may also be remotely managed using PowerShell Remoting. PowerShell Remoting must be performed over a HTTPS connection. The following article provides information about PowerShell Remoting:

- Running Remote Commands: <https://docs.microsoft.com/en-US/powershell/scripting/learn/remoting/running-remote-commands>

## 6.20 Managing apps and software restriction policies

 **Notes:**



## Microsoft Windows 10 GP OS Administrative Guidance

- Administrators must exercise discretion when installing apps based upon examining app metadata describing claimed capabilities. For example: Installing apps that declare the shareduserCertificates app capability allows the app to approve exceptions for shared use or destruction of keys/secrets that were imported by another app. For more information on app capabilities, see the topic App capability declarations: <https://docs.microsoft.com/en-us/windows/uwp/packaging/app-capability-declarations>.

### 6.20.1 Configuring with Windows Defender Application Control

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	All

Windows Defender Application Control (WDAC) is the recommended approach for setting software restriction policies in Windows. WDAC offers a variety of policies that can be implemented via Group Policy or MDM. See the following articles for an overview, design guidance, and implementation guidance:

- Windows Defender Application Control: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control>
- Deploy Windows Defender Application Control policies by using Group Policy: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/deploy-windows-defender-application-control-policies-using-group-policy>
- Deploy Windows Defender Application Control policies by using Microsoft Intune: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/deploy-windows-defender-application-control-policies-using-intune>

### 6.20.2 Configuring with AppLocker

<b>Role</b>	IT Administrator, Local Administrator
-------------	---------------------------------------



<b>Windows Editions</b>	Enterprise
-------------------------	------------

In addition to Windows Defender Application Control (WDAC), AppLocker may also be used to manage software restriction policies. As a best practice, organizations should use WDAC to enforce software restriction policies at the most restrictive level possible, and then use AppLocker to fine-tune the restrictions to an even lower level if needed. The following article provides more information on the relationship between WDAC and AppLocker:

- Windows Defender Device Guard with Applocker, including its relationship to WDAC: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-device-guard-and-applocker>

AppLocker policies may be configured locally via PowerShell or SecPol, or configured and deployed remotely via Group Policy. The scope of policies includes enabling or disabling access to the Microsoft Store. The following articles provide information on both local and remote options for AppLocker management:

- AppLocker Overview: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview>
- Administer AppLocker: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/administer-applocker>
- Use the AppLocker Windows PowerShell cmdlets: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/use-the-applocker-windows-powershell-cmdlets>
- Configure access to Microsoft Store: <https://docs.microsoft.com/en-us/windows/configuration/stop-employees-from-using-microsoft-store>

### 6.20.3 Configuring with enterprise app management and MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise



## Microsoft Windows 10 GP OS Administrative Guidance

IT Administrators may also configure some aspects of app management via MDM. The following article provides an overview of enterprise app management functionality in Windows:

- Enterprise app management: <https://docs.microsoft.com/en-us/windows/client-management/mdm/enterprise-app-management>

The EnterpriseModernAppManagement CSP is used to implement enterprise app management policies via MDM. The following article provides more information:

- EnterpriseModernAppManagementCSP: <https://docs.microsoft.com/en-us/windows/client-management/mdm/enterprisemodernappmanagement-csp>

### 6.20.4 Installing and uninstalling apps with the Windows user interface

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	All

Windows supports a wide variety of applications. Applications may be installed from the Microsoft Store, from installation media provided by app developers, or from installation files downloaded from the internet. The following article provides a summary of the options for installing applications in Windows:

- How to install programs on Windows 10: <https://support.microsoft.com/en-us/help/4026235/windows-10-how-to-install-programs>

The following article provides a summary of the options for removing applications from Windows:

- Repair or remove programs in Windows 10: <https://support.microsoft.com/en-us/help/4028054/windows-10-repair-or-remove-programs>



## 6.21 Developing applications

This section of the operational guidance is provided for application developers and is not related to the management functions that may be performed by the administrator or user roles described in the other sections of this document.

Developers may use Microsoft Visual Studio 2017 for development of applications. The following is a link to documentation for Microsoft Visual Studio 2017:

- Visual Studio : <https://docs.microsoft.com/en-us/visualstudio/ide/visual-studio-ide>

Applications developed in Microsoft Visual Studio 2017 will by default have the /GS flag set. The following is a link to documentation about the /GS flag in Microsoft Visual Studio:

- /GS (Buffer Security Check) : <https://docs.microsoft.com/en-us/cpp/build/reference/gs-buffer-security-check>

## 6.22 Managing self-test and health attestation

### **Note:**

- Windows automatically checks file integrity of files related to security functions. No configuration is necessary or possible.

### 6.22.1 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Pro, Enterprise

Health attestation policies can be managed to determine the health of enrolled Windows 10 and Windows Server devices using MDM. The following article provides details on the correct CSP to use to manage health attestation policies with MDM and to assess if an enrolled device has booted to a trusted and compliant state:



## Microsoft Windows 10 GP OS Administrative Guidance

- Device HealthAttestation CSP: <https://docs.microsoft.com/en-us/windows/client-management/mdm/healthattestation-csp>

### 6.22.2 Helper utility for health attestation logs

<b>Role</b>	Local Administrator
<b>Windows Editions</b>	All

The device will create a health attestation log every time the system boots. The logs are found in the following directory:

- %windir%\Logs\MeasuredBoot

The logs are in a binary format. To decode the logs, use the TPM Platform Crypto Provider and Toolkit utility, available for download from Microsoft here:

- TPM Platform Crypto Provider and Toolkit: <https://www.microsoft.com/en-us/download/details.aspx?id=52487&from=http%3A%2F%2Fresearch.microsoft.com%2Fen-us%2Fdownloads%2F74c45746-24ad-4cb7-ba4b-0c6df2f92d5d%2F>

### 6.23 Managing audit policy

<b>Role</b>	IT Administrator, Local Administrator
<b>Windows Editions</b>	All

This section provides more information for IT administrators on event auditing functionality in Windows, including solutions available to adjust logging scope and settings. This information is provided to enable IT Administrators to implement security monitoring and forensics required by their organization.



## Microsoft Windows 10 GP OS Administrative Guidance

The following log locations are always enabled:

- Windows Logs -> System
- Windows Logs -> Setup
- Windows Logs -> Security (for startup and shutdown of the audit functions and of the OS and kernel, and clearing the audit log)

For additional background on event logging and configuring audit policies in Windows, see these articles:

- Event types in Windows: <https://docs.microsoft.com/en-us/windows/win32/eventlog/event-types>
- Basic security audit policies: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/basic-security-audit-policies>
- Advanced security audit policies, including categories of audits in the Windows Security log: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing>
- Tips on filtering events in the Windows Event Viewer: <https://docs.microsoft.com/en-us/archive/blogs/rmilne/quick-tip-event-viewer-filtering>

### 6.23.1 Managing audit policy with the Auditpol command

The Auditpol command displays information about and performs functions to manipulate audit policies, including selecting events by attribute to audit. The following article provides an overview of the Auditpol command, including a list of all its commands and their syntax:

- Auditpol: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/auditpol>

The Auditpol set command sets the per-user audit policy, system audit policy, or auditing options. The following article provides information on how to use Auditpol set:

- Auditpol set: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/auditpol-set>



## Microsoft Windows 10 GP OS Administrative Guidance

For example, to enable all audits in the given subcategories of the Windows Logs -> Security log run the following commands at an elevated command prompt:

- Logon operations:

```
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
```

- Audit policy changes:

```
auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:enable
```

- IPsec operations:

```
auditpol /set /subcategory:"IPsec Main Mode" /success:enable /failure:enable
```

```
auditpol /set /subcategory:"IPsec Quick Mode" /success:enable /failure:enable
```

- Configuring IKEv1 and IKEv2 connection properties:

```
auditpol /set /subcategory:"Filtering Platform Policy Change" /success:enable /failure:enable
```

```
auditpol /set /subcategory:"Other Policy Change Events" /success:enable /failure:enable
```

- Registry changes (modifying TLS ciphersuite priority):

```
auditpol /set /subcategory:"Registry" /success:enable /failure:enable
```

### 6.23.2 Managing audit policy with the Secpol snap-in

The local security policy snap-in utility (secpol.msc) is used as an alternative to the auditpol utility for managing security policy settings, including audits. The following article provides information on administering security policy settings, including how to use the security policy snap-in:

- Administer security policy settings: <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/administer-security-policy-settings>



### 6.23.3 Managing audit policy with the Wevtutil utility

Wevtutil is a system utility that performs many of the management functions related to system and audit logs including the following:

- configure local audit storage capacity
- configure audit rules (includes enable/disable event logging for optional logging)
- enumerate the log names
- configure Analytic and Debug logs as enabled (e.g. Microsoft-Windows-CodeIntegrity/Verbose)

See the following article for more info on Wevtutil:

- Wevtutil: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil>

### 6.23.4 Retrieving and viewing audit logs using Get-WinEvent

The PowerShell Get-WinEvent cmdlet can be used to retrieve and view audit logs. For information on how to use Get-WinEvent, see the following article:

- Get-WinEvent <https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.diagnostics/get-winevent?view=powershell-6>

### 6.23.5 Configuring System Access Control Lists for audited objects

In addition to enabling audit policy as noted above, each registry key or file object to be audited must also have its auditing permissions set by changing the System Access Control List (SACL) for that object. The process is slightly different for each object type to be audited. For example, to set the SACL for a registry object:

1. Start the registry editor tool by executing the command regedit.exe as an administrator
2. Navigate to the registry path for the key that should be audited, right-click the key's node and select **Permissions...** on the key's context menu to open the **Permissions** dialog



## Microsoft Windows 10 GP OS Administrative Guidance

3. Click the **Advanced** button to open the **Advanced Security Settings** dialog, click on the **Auditing** tab and click the **Add** button to open the **Auditing Entry** dialog
4. Click the **Select a principal** to open the **Select User or Group** dialog to select a user (e.g. Administrator) and click the OK button.
5. Choose the desired audits using the **Type**, **Applies to** and **Basic Permissions** attributes and click **OK**
6. Click **OK** on the **Advanced Security Settings** dialog
7. Click OK on the **Permissions** dialog

For a file object, open the properties dialog for the file object, click **Security**, click **Advanced**, and click **Auditing**.

PowerShell may also be used to set the SACL on the file object using Powershell

- Get-Acl: <https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/get-acl?view=powershell-6>
- Set-Acl: <https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-acl?view=powershell-6>

For more information, the following TechNet article describes System Access Control Lists in general:

- Access Control Lists: <https://docs.microsoft.com/en-us/windows/desktop/secauthz/access-control-lists>



## 7 Audit events

This section provides a reference for the Windows audit records that can be used for security auditing and forensic investigation, as required for the Common Criteria evaluation. The event information for a collection of security functions are grouped together and then indexed under a heading that refers to the label in the Security Target. The log details, i.e. where an event is found and what its syntax in the log is, are included in a subsequent table and listed by event ID: [Events mapped to log details](#).

### 7.1 Audit events – GP OS protection profile

The following table lists the audit events from the GP OS protection profile and implemented by Windows. Refer to the table, [Events mapped to log details](#), for where to find each event within the Windows logs. All the events listed in this table are found in the Windows Security log.

Description	Context: Event ID (Detail) Note – <i>all</i> events are in the Security log.
Start-up and shut-down of the audit functions	Start-up: <b>4608</b> Shut-down: <b>1100</b>
Authentication events (Success/Failure)	Success: <b>4624</b> Failure: <b>4625</b>
Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes)	WRITE_DAC : <b>4670</b> All other object access writes : <b>4656</b>
Privilege or role escalation events (Success/Failure)	Success: <b>4673</b> Failure: <b>4674</b>



## Microsoft Windows 10 GP OS Administrative Guidance

File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions)	<b>4656</b>
User and Group management events (Successful and unsuccessful add, delete, modify, disable)	add user: <b>4720</b> add user to group: <b>4732</b> delete user: <b>4726</b> delete user from group: <b>4733</b> add group: <b>4731</b> delete group: <b>4734</b> modify group: <b>4735</b> modify user account: <b>4738</b> disable user: <b>4725</b>
Lock (disable) and unlock (re-enable) a user account	Lock: <b>4740</b> Unlock: <b>4767</b>
Audit and log data access events (Success/Failure)	Success, Failure: <b>4673</b>
Cryptographic verification of software (Success/Failure)	Failure: <b>3</b> Success: <b>2</b>
Program initiations (Success/Failure e.g. due to software restriction policy)	Success: <b>3038</b> (WDAC/Device Guard), <b>8020</b> (AppLocker) Failure: <b>3077</b> (WDAC/Device Guard) , <b>8022</b> (AppLocker)



Startup and shutdown of the RichOS and/or audit functions System reboot, restart, and shutdown events (Success/Failure),	Start-up: <b>4608</b> Shut-down: <b>1100</b>
Kernel module loading and unloading events (Success/Failure),	Success: <b>3038</b> (Other kernel modules), <b>Windows Boot Configuration Log</b> (Boot kernel module loading) Failure: <b>3004</b> (Other kernel modules), <b>Recovery Screen</b> (Boot kernel module loading)
Administrator or root-level access events (Success/Failure),	Success: <b>4624</b> Failure: <b>4625</b>

## 7.2 Audit events – WLAN client extended package

The following table lists the audit events from the WLAN Client Extended Package and implemented by Windows. Refer to the subsequent table, [Events mapped to log details](#), for guidance on where to find each event within the Windows logs.

Requirement	Auditable Events	Additional Audit Record Contents	Log Name: Event ID (Detail)
FAU_GEN.1/WLAN	None.		
FCS_CKM.1/WLAN	None.		
FCS_CKM.2/WLAN	None.		
FCS_CKM_EXT.4	None.		



# Microsoft Windows 10 GP OS Administrative Guidance

FCS_TLSC_EXT.1/WLAN	Failure to establish an EAP-TLS session.	Reason for failure	System: <b>36888</b> Microsoft-Windows-CAPI2/Operational: <b>11, 30</b>
	Establishment/termination of an EAP-TLS session.	Non-TOE endpoint of connection.	System: <b>36880</b> (Establishment) Microsoft-Windows-SChannel-Events/Perf: <b>1793</b> (Termination)
FIA_PAE_EXT.1	None.		
FMT_SMF_EXT.1/WLAN	None.		
FIA_X509_EXT.2/WLAN	None.		
FPT_TST_EXT.1/WLAN	Execution of this set of TSF self-tests.	[Selection: <i>The TSF binary file that caused the integrity violation</i> ].	System: <b>20</b>
	[Selection: <i>detected integrity violation</i> ].		



FTA_WSE_EXT.1	All attempts to connect to access points.	Identity of access point being connected to as well as success and failures (including reason for failure).	Microsoft-Windows-WLAN-AutoConfig/Operational log event: <b>8001</b> (successful WLAN connection) <b>8002</b> (WLAN connection failure) <b>8003</b> (successful WLAN disconnection) <b>11004</b> (wireless network blocked) <b>11005</b> (wireless security succeeded) <b>11006</b> (wireless security failed) <b>12013</b> (failure due to user account)
FTP_ITC_EXT.1/WLAN	All attempts to establish a trusted channel.	Identification of the non-TOE endpoint of the channel.	EAP-TLS/802.1x/802.11-2012: Microsoft-Windows-WLAN-AutoConfig/Operational: <b>8001, 8003</b>

## 7.3 Audit events – IPsec Extended Package

The following table lists the audit events from the IPSec Extended Package and implemented by Windows. Refer to the subsequent table, [Events mapped to log details](#), for guidance on where to find each event within the Windows logs.

Requirement / Management Function	Auditable Events	Additional Audit Record Contents	Log Name: Event ID (Detail)
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	None	Windows Logs/Security: <b>4719</b>



# Microsoft Windows 10 GP OS Administrative Guidance

FCS_IPSEC_EXT.1	<ul style="list-style-type: none"> <li>Decisions to DISCARD, BYPASS, PROTECT network packets processed by the TOE.</li> <li>Failure to establish an IPsec SA.</li> <li>Establishment/Termination of an IPsec SA.</li> </ul>	<ul style="list-style-type: none"> <li>Presumed identity of source subject.</li> <li>Identity of destination subject.</li> <li>Transport layer protocol, if applicable.</li> <li>Source subject service identifier, if applicable.</li> <li>The entry in the SPD that applied to the decision.</li> <li>Reason for failure.</li> <li>Non-TOE endpoint of connection (IP address) for both successes and failures.</li> </ul>	<p>Windows Logs/Security:</p> <p>DISCARD, BYPASS, AND PROTECT – see <b>5152, 5156, 5157</b></p> <p>Failure to establish an SA – see <b>4653, 4654</b></p> <p>Establishment / termination of an SA – see <b>4650, 4655, 5451, 5452</b></p> <ul style="list-style-type: none"> <li></li> </ul>
FIA_PSK_EXT.1	None, as the randomized pre-shared key is not supported	N/A	N/A
FMT_SMF.1 – any VPN configuration change	Success or failure of the management function.	None	Microsoft-Windows-VPN-Client/Operational: 10001 (success), 10002 (failure).
FMT_SMF.1 / Specify VPN gateways to use for connections	Success or failure of the management function.	None	Windows Logs/Security: <b>5043</b>
FMT_SMF.1 / Specify client credentials to be used for connections	Success or failure of the management function.	None	Windows Logs/Security: <b>5040</b>
FMT_SMF.1 / Configuration of IKE protocol version(s) used	Success or failure of the management function.	None	Windows Logs/Security: <b>5043</b>



## Microsoft Windows 10 GP OS Administrative Guidance

FMT_SMF.1 / Configure IKE authentication techniques used	Success or failure of the management function.	None	Windows Logs/Security: <b>5040</b>
FMT_SMF.1 / Configure the cryptoperiod for the established session keys.	Success or failure of the management function.	None	N/A – The cryptoperiod is configured on the VPN Gateway
FMT_SMF.1 / Configure certificate revocation check	Success or failure of the management function.	None	Windows Logs/Security: <b>4950</b>
FMT_SMF.1 / Specify the algorithm suites that may be proposed and accepted during the IPsec exchanges	Success or failure of the management function.	None	Windows Logs/Security: <b>5046</b>
FMT_SMF.1 / Load X.509v3 certificates used by the security functions in this PP	Success or failure of the management function.	None	Applications and Services Logs- >Microsoft-> Windows- >CertificateServicesClient-Lifecycle-User- >Operational: <b>1006</b>
FMT_SMF.1 / Ability to update the TOE, and to verify the updates,	Success or failure of the management function.	None	Windows Logs/Setup: <b>1, 2, 3</b>
FPT_TST_EXT.1 (IPSEC)	Violation of code integrity policy	None	Application and Services Logs- >Microsoft->Windows->CodeIntegrity- >Operational: <b>3033, 3076, 3077</b>



## 7.4 Events mapped to log details

The following table maps the event IDs referenced in the preceding tables to specific Windows logs, including details on where to find the information in the log, the specific log message, and the fields included. The fields in the table refer to the hierarchical field names used in Event Viewer event data, on the Details tab, when the Friendly View radio button is selected. The field names also correspond to the node names in XML files provided as evidence. The Message values correspond to the message displayed in the General tab.

Event ID	Log Location	Message	Fields
1	Windows Logs->Setup	Initiating changes for package	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Security[UserID]:</b> <Subject identifier > <b>System-&gt;Level:</b> <Outcome as Success or Failure>
2	Windows Logs -> System	Package was successfully changed to the Installed state	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Security[UserID]:</b> <Subject identifier > <b>System-&gt;Level:</b> <Outcome as Success or Failure>
3	Windows Logs->Setup	Windows update could not be installed because ... "The data is invalid"	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Security[UserID]:</b> <Subject identifier > <b>System-&gt;Level:</b> <Outcome as Success or Failure>
11	Microsoft-Windows-CAPI2/Operational	Build Chain	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identity> <b>UserData-&gt;Result:</b> <Reason for failure of validation>



20	Windows Logs -> System	The last boot's success was <LastBootGood event data>.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <type of event> <b>System-&gt; Security[UserID]:</b> <subject identifier >  <b>EventData-&gt;LastBootGood:</b> <Outcome as true or false indicating if the kernel-mode cryptographic self-tests and RNG initialization succeeded or failed>
30	Microsoft-Windows-CAPI2/Operational	Verify Chain Policy	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identity> <b>UserData-&gt;CertVerifyCertificateChainPolicy-&gt;Certificate:</b> <Issuer Name and Subject Name of certificate>
1006	<b>Applications and Services Logs-&gt; Microsoft-&gt;Windows-&gt;CertificateServicesClient-Lifecycle-User -&gt; Operational</b>  <b>Applications and Services Logs -&gt; Microsoft -&gt; Windows -&gt; CertificateServicesClient-Lifecycle-System -&gt; Operational</b>	A new certificate has been installed.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identifier>
1100	Windows Logs->Setup	The event logging service has shut down	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>N/A:</b> <Subject identifier>



1793	Microsoft-Windows-SChannel-Events/Perf	A TLS Security Context handle is being deleted	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <type of event> <b>System-&gt; Security[UserID]:</b> <subject identifier > <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>EventData-&gt;ContextHandle:</b> <non-TOE endpoint>
3004	Application and Services Logs->Microsoft->Windows->CodeIntegrity	Windows is unable to verify the image integrity of the file <pathname> because the file hash could not be found on the system.	Subcategory: Security State Change
3033	Application and Services Logs->Microsoft->Windows->CodeIntegrity->Operational	Code Integrity determined that a process <process name> attempted to load <executable file name> that did not meet the Enterprise signing level requirements	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identifier>
3038	Application and Services Logs->Microsoft->Windows->CodeIntegrity->Verbose	Code Integrity started validating image header of <kernel module pathname> file	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identifier>



# Microsoft Windows 10 GP OS Administrative Guidance

3076	<b>Application and Services Logs-&gt;Microsoft-&gt;Windows-&gt;CodeIntegrity-&gt;Operational</b>	Code Integrity determined that a process <process name> attempted to load <target process name> that did not meet the Enterprise signing level requirements or violated code integrity policy. <policy ID>. However, due to code integrity auditing policy, the image was allowed to load.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identifier>
3077	<b>Application and Services Logs-&gt;Microsoft-&gt;Windows-&gt;CodeIntegrity-&gt;Operational</b>	Code Integrity determined that a process <process name> attempted to load <target process name> that did not meet the Enterprise signing level requirements or violated code integrity policy. <policy ID>.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identifier>
4608	<b>Windows Logs-&gt;Security</b>  Subcategory: Security State Change	Startup of audit functions	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>N/A:</b> <Subject identifier>



<b>4624</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: Logon	An account was successfully logged on.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;TargetUserSid:</b> <Subject identifier>
<b>4625</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: Logon	An account failed to log on.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;TargetUserSid:</b> <Subject identifier>
<b>4650</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: IPsec Main Mode	IPsec main mode security association was established. {Mode and authentication details.}	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>System-&gt;Computer:</b> <Subject identifier> <b>EventData-&gt;RemoteMMPrincipalName:</b> <Presumed identity of source subject> <b>EventData-&gt;RemoteAddress</b> <Non-TOE endpoint of connection> <b>EventData-&gt;LocalMMPrincipalName:</b> <Identity of destination subject> <b>N/A:</b> <Transport layer protocol> <b>EventData-&gt;MMFilterID:</b> <The entry in the SPD that applied to the decision> <b>N/A:</b> <Reason for failure>



# Microsoft Windows 10 GP OS Administrative Guidance

4651	<b>Windows Logs-&gt;Security</b>  Subcategory: IPsec Main Mode	IPsec main mode security association was established. A certificate was used for authentication.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>System-&gt;Computer:</b> <Subject identifier> <b>EventData-&gt;RemoteMMPrincipalName:</b> <Presumed identity of source subject> <b>EventData-&gt;RemoteAddress</b> <Non-TOE endpoint of connection> <b>EventData-&gt;LocalMMPrincipalName:</b> <Identity of destination subject> <b>N/A:</b> <Transport layer protocol> <b>EventData-&gt;MMFilterID:</b> <The entry in the SPD that applied to the decision> <b>N/A:</b> <Reason for failure>
4652	<b>Windows Logs -&gt; Security</b>  IPsec Main Mode	IPsec main mode negotiation failed	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>System-&gt;Computer:</b> <Subject identifier> <b>EventData-&gt;RemoteMMPrincipalName:</b> <Presumed identity of source subject> <b>EventData-&gt;RemoteAddress</b> <Non-TOE endpoint of connection> <b>EventData-&gt;LocalMMPrincipalName:</b> <Identity of destination subject> <b>N/A:</b> <Transport layer protocol> <b>EventData-&gt;MMFilterID:</b> <The entry in the SPD that applied to the decision> <b>EventData-&gt;FailureReason:</b> <Reason for failure>



<p><b>4653</b></p>	<p><b>Windows Logs -&gt; Security</b></p> <p>IPsec Main Mode</p>	<p>IPsec main mode negotiation failed</p>	<p><b>System-&gt;TimeCreated[SystemTime]:</b> &lt;Date and time of event&gt;</p> <p><b>System-&gt;Task:</b> &lt;Type of event&gt;</p> <p><b>System-&gt;Keywords:</b> &lt;Outcome as Success or Failure&gt;</p> <p><b>System-&gt;Computer:</b> &lt;Subject identifier&gt;</p> <p><b>EventData-&gt;RemoteMMPrincipalName:</b> &lt;Presumed identity of source subject&gt;</p> <p><b>EventData-&gt;RemoteAddress</b>&lt;Non-TOE endpoint of connection&gt;</p> <p><b>EventData-&gt;LocalMMPrincipalName:</b> &lt;Identity of destination subject&gt;</p> <p><b>N/A:</b> &lt;Transport layer protocol&gt;</p> <p><b>EventData-&gt;MMFilterID:</b> &lt;The entry in the SPD that applied to the decision&gt;</p> <p><b>EventData-&gt;FailureReason:</b>&lt;Reason for failure&gt;</p>
<p><b>4654</b></p>	<p><b>Windows Logs -&gt; Security</b></p> <p>IPsec Quick Mode</p>	<p>IPsec quick mode negotiation failed</p>	<p><b>System-&gt;TimeCreated[SystemTime]:</b> &lt;Date and time of event&gt;</p> <p><b>System-&gt;Task:</b> &lt;Type of event&gt;</p> <p><b>System-&gt;Keywords:</b> &lt;Outcome as Success or Failure&gt;</p> <p><b>System-&gt;Computer:</b> &lt;Subject identifier&gt;</p> <p><b>EventData-&gt;RemoteAddress, RemotePort:</b> &lt;Presumed identity of source subject&gt; &lt;Non-TOE endpoint of connection&gt;</p> <p><b>EventData-&gt;LocalAddress,LocalPort:</b> &lt;Identity of destination subject&gt;</p> <p><b>EventData-&gt;Protocol:</b> &lt;Transport layer protocol&gt;</p> <p><b>EventData-&gt;QMFilterID,MMSAID,TunnelId:</b> &lt;The entry in the SPD that applied to the decision&gt;</p> <p><b>EventData-&gt;FailureReason:</b>&lt;Reason for failure&gt;</p>



<b>4655</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: IPsec Main Mode	IPsec main mode security association ended	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>System-&gt;Computer:</b> <Subject identifier> <b>EventData-&gt;RemoteAddress</b> <Non-TOE endpoint of connection> <b>EventData-MMSAID:</b> <Presumed identity of source subject> <Identity of destination subject> <The entry in the SPD that applied to the decision> <b>N/A:</b> <Transport layer protocol> <b>N/A:</b> <Reason for failure>
<b>4656</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: Handle Manipulation	A handle to an object was requested.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4670</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: Policy Change	Permissions on an object were changed.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4673</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: Sensitive Privilege Use	A privileged service was called.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4674</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: Sensitive Privilege Use	An operation was attempted on a privileged object.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>



<b>4720</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: User Account Management	A user account was created.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4725</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: User Account Management	A user account was disabled.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4726</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: User Account Management	A user account was deleted.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4719</b>	<b>Windows Logs -&gt; Security</b>  Subcategory: Audit Policy Change	System audit policy was changed	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData -&gt;SubjectUserSid:</b> <Subject identifier >
<b>4731</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: User Account Management	A security-enabled local group was created.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4732</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: User Account Management	A member was added to a security-enabled group.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>



# Microsoft Windows 10 GP OS Administrative Guidance

<b>4733</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: User Account Management	A member was removed from a security-enabled group.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4734</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: User Account Management	A security-enabled local group was deleted.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4735</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: User Account Management	A security-enabled local group was changed.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4738</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: User Account Management	A user account was changed	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4740</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: Account Lockout	A user account was locked out.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>
<b>4767</b>	<b>Windows Logs-&gt;Security</b>  Subcategory: Account Lockout	A user account was unlocked.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;SubjectUserSid:</b> <Subject identifier>



# Microsoft Windows 10 GP OS Administrative Guidance

<b>4950</b>	<b>Windows Logs-&gt;Security</b> Subcategory: MPSSVC Rule-Level Policy Change	A Windows Firewall setting has changed.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>System-&gt;Computer:</b> <Subject identifier>
<b>5040</b>	<b>Windows Logs-&gt;Security</b> Subcategory: Filtering Platform Policy Change	A change was made to IPsec settings. An authentication set was added.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>System-&gt;Computer:</b> <Subject identifier>
<b>5043</b>	<b>Windows Logs-&gt;Security</b> Subcategory: Filtering Platform Policy Change	A change was made to IPsec settings. A connection security rule was added.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>System-&gt;Computer:</b> <Subject identifier>
<b>5046</b>	<b>Windows Logs-&gt;Security</b> Subcategory: Filtering Platform Policy Change	A change was made to IPsec settings. A crypto set was added.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>System-&gt;Computer:</b> <Subject identifier>
<b>5152</b>	<b>Windows Logs-&gt;Security</b> Filtering Platform Packet Blocked	The Windows Filtering Platform has blocked a packet.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;ProcessId, Application:</b> <Subject identifier> <b>EventData-&gt;SourceAddress,SourcePort:</b> <Presumed identity of source subject> <Non-TOE endpoint of connection> <b>EventData-&gt;DestAddress, DestPort:</b> <Identity of destination subject> <b>EventData-&gt;Protocol:</b> <Transport layer protocol> <b>EventData-&gt;FilterRTID, LayerName, LayerRTID:</b> <The entry in the SPD that applied to the decision> <Reason for failure>



5156	<b>Windows Logs-&gt;Security</b>  Filtering Platform Connection	The Windows Filtering Platform has permitted a connection	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;ProcessId, Application:</b> <Subject identifier> <b>EventData-&gt;SourceAddress,SourcePort:</b> <Presumed identity of source subject> <Non-TOE endpoint of connection> <b>EventData-&gt;DestAddress,DestPort:</b> <Identity of destination subject> <b>EventData-&gt;Protocol:</b> <Transport layer protocol> <b>EventData-&gt;FilterRTID,LayerName,LayerRTID:</b> <The entry in the SPD that applied to the decision> <Reason for failure>
5157	<b>Windows Logs-&gt;Security</b>  Filtering Platform Connection Blocked	The Windows Filtering Platform has blocked a connection.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Task:</b> <Type of event> <b>System-&gt;Keywords:</b> <Outcome as Success or Failure> <b>EventData-&gt;ProcessId, Application:</b> <Subject identifier> <b>EventData-&gt;SourceAddress,SourcePort:</b> <Presumed identity of source subject> <Non-TOE endpoint of connection> <b>EventData-&gt;DestAddress,DestPort:</b> <Identity of destination subject> <b>EventData-&gt;Protocol:</b> <Transport layer protocol> <b>EventData-&gt;FilterRTID,LayerName,LayerRTID:</b> <The entry in the SPD that applied to the decision> <Reason for failure>



5451	<b>Windows Logs-&gt;Security</b>  Subcategory: IPsec Quick Mode	IPsec quick mode security association was established	<p><b>System-&gt;TimeCreated[SystemTime]:</b> &lt;Date and time of event&gt;</p> <p><b>System-&gt;Task:</b> &lt;Type of event&gt;</p> <p><b>System-&gt;Keywords:</b> &lt;Outcome as Success or Failure&gt;</p> <p><b>System-&gt;Computer:</b> &lt;Subject identifier&gt;</p> <p><b>EventData-&gt;MainModeSaid</b> &lt;Presumed identity of source subject&gt;</p> <p><b>EventData-&gt;RemoteAddress, RemotePort:</b> &lt;Non-TOE endpoint of connection&gt;</p> <p><b>EventData-&gt; MainModeSaid,LocalAddress,LocalPort:</b> &lt;Identity of destination subject&gt;</p> <p><b>EventData-&gt;IpProtocol:</b> &lt;Transport layer protocol&gt;</p> <p><b>EventData-&gt;TunnelFilerId,TunnelId:</b> &lt;The entry in the SPD that applied to the decision&gt;</p> <p><b>N/A:</b>&lt;Reason for failure&gt;</p>
5452	<b>Windows Logs-&gt;Security</b>  Subcategory: IPsec Quick Mode	IPsec quick mode security association ended	<p><b>System-&gt;TimeCreated[SystemTime]:</b> &lt;Date and time of event&gt;</p> <p><b>System-&gt;Task:</b> &lt;Type of event&gt;</p> <p><b>System-&gt;Keywords:</b> &lt;Outcome as Success or Failure&gt;</p> <p><b>System-&gt;Computer:</b> &lt;Subject identifier&gt;</p> <p><b>EventData-&gt;QuickModeSaid</b> &lt;Presumed identity of source subject&gt;</p> <p><b>EventData-&gt;RemoteAddress, RemotePort:</b> &lt;Non-TOE endpoint of connection&gt;</p> <p><b>EventData-&gt; QuickModeSaid,LocalAddress,LocalPort:</b> &lt;Identity of destination subject&gt;</p> <p><b>EventData-&gt;IpProtocol:</b> &lt;Transport layer protocol&gt;</p> <p><b>EventData-&gt;TunnelId,TrafficSelectorId:</b> &lt;The entry in the SPD that applied to the decision&gt;</p> <p><b>N/A:</b>&lt;Reason for failure&gt;</p>



8001	<b>Microsoft-Windows-WLAN-AutoConfig/Operational</b>	WLAN AutoConfig service has successfully connected to a wireless network	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identity> <b>EventData-&gt;PHYType, AuthenticationAlgorithm:</b> <Trusted channel protocol> <b>EventData-&gt;SSID:</b> <Non-TOE endpoint of connection>
8002	<b>Microsoft-Windows-WLAN-AutoConfig/Operational</b>	WLAN AutoConfig service failed to connect to a wireless network	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identity> <b>EventData-&gt;PHYType, AuthenticationAlgorithm:</b> <Trusted channel protocol> <b>EventData-&gt;SSID:</b> <Non-TOE endpoint of connection>
8003	<b>Microsoft-Windows-WLAN-AutoConfig/Operational</b>	WLAN AutoConfig service has successfully disconnected from a wireless network	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identity> <b>EventData-&gt;ConnectionId:</b> <Trusted channel protocol> <b>EventData-&gt;SSID:</b> <Non-TOE endpoint of connection>
8020	<b>Application and Services Logs-&gt;Microsoft-&gt;Windows-&gt;AppLocker-&gt;Packaged app-Execution</b>	<Packaged app name> was allowed to run.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identifier>
8022	<b>Application and Services Logs-&gt;Microsoft-&gt;Windows-&gt;AppLocker-&gt;Packaged app-Execution</b>	<Packaged app name> was prevented from running.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identifier>



<b>10001</b>	<b>Microsoft-Windows-VPN-Client/Operational</b>	VPN Profile {Name} has been created with the following properties: {Properties}	<b>TimeCreated[SystemTime]:</b> <Date and time of event> <b>Provider[Name]:</b> <Provider name> <b>OpcodeDisplayName:</b> <Success or failure> <b>Properties:</b> <Properties>
<b>10002</b>	<b>Microsoft-Windows-VPN-Client/Operational</b>	VPN Profile {Name} could not be created. {Error ID} {Connection Properties}	<b>TimeCreated[SystemTime]:</b> <Date and time of event> <b>Provider[Name]:</b> <Provider name> <b>OpcodeDisplayName:</b> <Success or failure> <b>Properties:</b> <Properties>
<b>11004</b>	<b>Microsoft-Windows-WLAN-AutoConfig/Operational</b>	Wireless security stopped.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identity> <b>EventData-&gt;SSID:</b> <Non-TOE endpoint of connection>
<b>11005</b>	<b>Microsoft-Windows-WLAN-AutoConfig/Operational</b>	Wireless security succeeded.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identity> <b>EventData-&gt;SSID:</b> <Non-TOE endpoint of connection>
<b>11006</b>	<b>Microsoft-Windows-WLAN-AutoConfig/Operational</b>	Wireless security failed.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identity> <b>EventData-&gt;SSID:</b> <Non-TOE endpoint of connection> <b>EventData-&gt;ReasonText:</b> <Failure condition> <b>EventData-&gt;ReasonCode:</b> <Failure condition error code>



<b>12013</b>	<b>Microsoft-Windows-WLAN-AutoConfig/Operational</b>	Wireless 802.1x authentication failed.	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <Type of event> <b>System-&gt;Level:</b> <Outcome as Success or Failure> <b>System-&gt;Security[UserID]:</b> <Subject identity> <b>EventData-&gt;SSID:</b> <Non-TOE endpoint of connection>
<b>36880</b>	<b>Windows Logs -&gt; System</b>	An TLS server handshake completed successfully. The negotiated cryptographic parameters are as follows:	<b>System-&gt;TimeCreated[SystemTime]:</b> <Date and time of event> <b>System-&gt;Provider[Name]:</b> <type of event> <b>System-&gt;Security[UserID]:</b> <subject identifier > <b>UserData-&gt;EventXML-&gt;TargetName:</b> <Non-TOE endpoint>



36888	Windows Logs -> System	<p>A fatal alert was generated and sent to the remote endpoint. This may result in termination of the connection. The TLS protocol defined fatal error code is %1.</p>	<p><b>System-&gt;TimeCreated[SystemTime]:</b> &lt;Date and time of event&gt;  <b>System-&gt;Provider[Name]:</b> &lt;type of event&gt;  <b>System-&gt;Security[UserID]:</b> &lt;subject identifier &gt;  <b>UserData-&gt;EventXML-&gt;TargetName:</b> &lt;Non-TOE endpoint &gt;  <b>UserData-&gt;EventXML-&gt;AlertDesc:</b> &lt; Reason for failure&gt;  <b>UserData-&gt;EventXML-&gt;ErrorState:</b> &lt; Reason for failure &gt;</p> <p>The following are the possible error codes:</p> <ul style="list-style-type: none"> <li>10 Unexpected message</li> <li>20 Bad record MAC</li> <li>22 Record overflow</li> <li>30 Decompression fail</li> <li>40 Handshake failure</li> <li>47 Illegal parameter</li> <li>48 Unknown CA</li> <li>49 Access denied</li> <li>50 Decode error</li> <li>51 Decrypt error</li> <li>70 Protocol version</li> <li>71 Insufficient security</li> <li>80 Internal error</li> <li>110 Unsupported extension</li> </ul>
-------	------------------------	--	--



## 8 Configuration Annex

This section provides guidance for IT administrators who manage systems that must meet the requirements of the Configuration Annex to the Protection Profile (PP) for General Purpose Operating Systems (GPOS). The guidance is aligned with the following version of the Configuration Annex:

- Configuration Annex Release 1 for PP GPOS version 4.2, [https://www.niap-ccevs.org/MMO/PP/PP\\_OS-v4.2\\_configannex.pdf](https://www.niap-ccevs.org/MMO/PP/PP_OS-v4.2_configannex.pdf)

### 8.1 Supported Configuration Actions

The following table lists the Configuration Actions supported by Windows. For each action, the table lists the methods available in Windows to configure it and a reference to the section of this Operational and Administrative Guide with implementation instructions.

Configuration Action	NIST Control Reference	GP OS SFR	Specific Value for DoD or CNSSI 1253 (If Published)	Windows Management Method(s)	Admin Guide Reference
Configure Minimum Password Length to 12 Characters	IA-5 (1)(a)	FMT_MOF_EXT.1	12 characters	MDM Group Policy Command Line	6.8 Managing passwords and password policy
Require at Least 1 Special Character in Password	IA-5 (1)(a)	FMT_MOF_EXT.1	At least one	MDM Group Policy	6.8 Managing passwords and password policy
Require at Least 1 Numeric Character in Password	IA-5 (1)(a)	FMT_MOF_EXT.1	At least one	MDM Group Policy	6.8 Managing passwords and password policy
Require at Least 1 Uppercase Character in Password	IA-5 (1)(a)	FMT_MOF_EXT.1	At least one	MDM Group Policy	6.8 Managing passwords and password policy



# Microsoft Windows 10 GP OS Administrative Guidance

Configuration Action	NIST Control Reference	GP OS SFR	Specific Value for DoD or CNSSI 1253 (If Published)	Windows Management Method(s)	Admin Guide Reference
Require at Least 1 Lowercase Character in Password	IA-5 (1)(a)	FMT_MOF_EXT.1	At least one	MDM Group Policy	6.8 Managing passwords and password policy
Enable Screen Lock	AC-11a	FMT_MOF_EXT.1		MDM Group Policy	6.11 Managing screen lock and session timeout
Set Screen Lock Timeout Period to 30 Minutes or Less	AC-11a	FMT_MOF_EXT.1	30 minutes	MDM Group Policy	6.11 Managing screen lock and session timeout
Disable Unauthenticated Login (such as Guest Accounts)	AC-11a	FIA_AFL.1		MDM Group Policy	6.8 Managing passwords and password policy
Set Maximum Number of Authentication Failures to 3 Within 15 Minutes	AC-7a	FMT_MOF_EXT.1	3 failures 15 minutes	MDM Group Policy Command Line	6.8 Managing passwords and password policy
Enable Host-Based Firewall	SC-7(12)	FMT_MOF_EXT.1		PowerShell	6.16 Managing the firewall
Configure Name/Address of Remote Management Server from Which to Receive Config Settings	CM-3(3)	FMT_MOF_EXT.1		MDM Group Policy	3.6 Modern device management 3.7 Approaches for configuring Windows policies
Configure the System to Offload Audit Records to a Log Server	AU-4(1)	FAU_GEN.1.1.c		<i>Not in scope for this GPOS evaluation per the Security Target.</i>	



Configuration Action	NIST Control Reference	GP OS SFR	Specific Value for DoD or CNSSI 1253 (If Published)	Windows Management Method(s)	Admin Guide Reference
Set Logon Warning Banner	AC-8a	FMT_MOF_EXT.1	See text below	MDM Group Policy Registry	6.12 Managing the logon banner
Audit All Logons (Success/Failure) and Logoffs (Successful)	AU-2a	FAU_GEN.1.1.c	Authentication events: (1) Logons (Success/Failure) (2) Logoffs (Success)	Group Policy Command Line	6.23 Managing audit policy
Audit File and Object Events (Unsuccessful)	AU-2a	FAU_GEN.1.1.c	File and object events: (1) Create (Success/Failure) (2) Access (Success/Failure) (3) Delete (Success/Failure) (4) Modify (Success/Failure) (5) Permission Modification (Success/Failure) (6) Ownership Modification (Success/Failure)	Group Policy Command Line	6.23 Managing audit policy



# Microsoft Windows 10 GP OS Administrative Guidance

Configuration Action	NIST Control Reference	GP OS SFR	Specific Value for DoD or CNSSI 1253 (If Published)	Windows Management Method(s)	Admin Guide Reference
Audit User and Group Management Events (Success/Failure)	AU-2a	FAU_GEN.1.1.c	User and group management events: (1) User add, delete, modify, disable, enable (Success/Failure) (2) Group/Role add, delete, modify (Success/Failure)	Group Policy Command Line	6.23 Managing audit policy
Audit Privilege or Role Escalation Events (Success/Failure)	AU-2a	FAU_GEN.1.1.c	Privilege/Role escalation (Success/Failure)	Group Policy Command Line	6.23 Managing audit policy
Audit All Audit and Log Data Accesses (Success/Failure)	AU-2a	FAU_GEN.1.1.c	Audit and log data access (Success/Failure)	Group Policy Command Line	6.23 Managing audit policy
Audit Cryptographic Verification of Software (Success/Failure)	AU-2a	FAU_GEN.1.1.c		Group Policy Command Line	6.23 Managing audit policy
Audit Program Initiations (Success/Failure)	AU-2a	FAU_GEN.1.1.c	Application (e.g., Firefox, Internet Explorer, MS Office Suite, etc.) initialization (Success/Failure)	Group Policy Command Line	6.23 Managing audit policy



Configuration Action	NIST Control Reference	GP OS SFR	Specific Value for DoD or CNSSI 1253 (If Published)	Windows Management Method(s)	Admin Guide Reference
Audit System Reboot, Restart, and Shutdown Events (Success/Failure)	AU-2a	FAU_GEN.1.1.c	System reboot, restart and shutdown (Success/Failure)	Group Policy Command Line	6.23 Managing audit policy
Audit Kernel Module Loading and Unloading Events (Success/Failure)	AU-2a	FAU_GEN.1.1.c		Group Policy Command Line	6.23 Managing audit policy
Enable Automatic Software Update	SI-2	FMT_MOF_EXT.1		MDM Group Policy Command Line Windows GUI	6.14 Managing updates

## 8.1.1 Logon banner text

The following text is the value specified for the logon banner, copied here from the published Configuration Annex for convenience.

### 8.1.1.1 For DoD Systems:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.



## Microsoft Windows 10 GP OS Administrative Guidance

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

### 8.1.1.2 For non-DoD NSS:

Organization-defined system use notification message or banner.