

# Operational and Administrative Guidance

## Microsoft Windows 10 and Windows Server

Common Criteria Evaluation for  
Microsoft Windows 10 and Windows Server Version 1803

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.

© 2018 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.

# 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	Mobile device management.....	12
3.7	Approaches for configuring Windows policies .....	13
3.7.1	Setting policies with mobile device management (MDM):.....	13
3.7.2	Setting policies with Group Policy Objects (GPO):.....	13
3.7.3	Setting policies with PowerShell scripts:.....	14
4	Evaluated editions and platforms .....	14
5	Evaluated configuration.....	15
5.1	Installing the operating system.....	15
5.2	Operational prerequisites.....	16
5.2.1	Trusted platforms .....	16
5.2.2	Device administration .....	16
5.2.3	Security updates.....	16
5.2.4	Mode of operation.....	17
5.2.5	FIPS 140 cryptography mode.....	17
5.2.6	Additional cryptography configuration.....	18
5.2.7	Device access.....	19
6	Managing evaluated features.....	19
6.1	Managing cryptography .....	19

## Microsoft Windows 10 GP OS Administrative Guidance

6.2	Managing X.509 certificates .....	20
6.2.1	Client certificates and Certificate Authorities.....	20
6.2.2	Root certificates.....	21
6.2.3	Certificate name comparison .....	22
6.2.4	Certificate validation.....	22
6.3	Managing Transport Layer Security (TLS).....	24
6.3.1	Available ciphersuites.....	24
6.3.2	Available TLS-EAP ciphersuites.....	25
6.3.3	Configuring with MDM.....	26
6.3.4	Configuring with group policy.....	26
6.3.5	Configuring with PowerShell .....	27
6.3.6	Generating X.509 certificates with templates .....	27
6.3.7	Managing signature algorithms with the Windows registry .....	28
6.3.8	Choosing TLS in a web browser .....	28
6.4	Managing network connections .....	29
6.4.1	Enabling or disabling network connections with the Windows UI .....	29
6.4.2	Enabling or disabling network connections with PowerShell .....	29
6.4.3	Configuring Wi-Fi access with MDM.....	29
6.4.4	Configuring Wi-Fi access with the Windows user interface .....	30
6.4.5	Configuring allowed Wi-Fi networks with MDM .....	30
6.4.6	Configuring allowed Wi-Fi networks with Group Policy .....	30
6.4.7	Selecting a secure Wi-Fi connection with the Windows UI .....	31
6.4.8	Configuring a Wi-Fi connection profile with the Windows UI.....	31
6.5	Managing personal hotspots.....	32
6.5.1	Configuring with MDM.....	32
6.5.2	Configuring with group policy.....	33

## Microsoft Windows 10 GP OS Administrative Guidance

6.5.3	Configuring with the Windows user interface .....	33
6.6	Managing Bluetooth .....	33
6.6.1	Configuring Bluetooth adapters with MDM.....	34
6.6.2	Enabling or disabling Bluetooth adapters with the Windows UI.....	34
6.6.3	Enabling or disabling Bluetooth adapters with PowerShell .....	34
6.7	Managing passwords and password policy.....	35
6.7.1	Configuring with MDM.....	35
6.7.2	Configuring with group policy.....	35
6.7.3	Configuring with net accounts utility.....	35
6.8	Managing smart card logon.....	36
6.9	Managing Windows Hello.....	36
6.9.1	Configuring biometric authentication with the Windows UI .....	36
6.9.2	Configuring PIN authentication with group policy.....	37
6.9.3	Configuring PIN authentication with the Windows UI .....	37
6.10	Managing screen lock and session timeout.....	38
6.10.1	Configuring with MDM .....	38
6.10.2	Configuring with group policy .....	38
6.10.3	Configuring with the Windows registry.....	39
6.10.4	Configuring with the Windows user interface.....	39
6.11	Managing the logon banner .....	40
6.11.1	Configuring with MDM .....	40
6.11.2	Configuring with group policy .....	40
6.11.3	Configuring with the Windows registry.....	40
6.12	Managing USB.....	41
6.12.1	Configuring with the Windows UI.....	41
6.12.2	Configuring with PowerShell.....	41

## Microsoft Windows 10 GP OS Administrative Guidance

6.12.3	Configuring with the Windows registry.....	42
6.13	Managing updates.....	42
6.13.1	Configuring using MDM.....	42
6.13.2	Configuring using group policy.....	43
6.13.3	Configuring using the Server Configuration tool.....	43
6.13.4	Checking for OS updates using the Windows UI.....	43
6.13.5	Installing Windows updates via the command line .....	44
6.13.6	Checking for Windows Store application updates .....	44
6.14	Managing the firewall.....	44
6.14.1	Configuring with PowerShell.....	44
6.15	Managing domains.....	45
6.15.1	Configuring with PowerShell.....	45
6.16	Managing date and time .....	45
6.16.1	Configuring with PowerShell.....	45
6.16.2	Configuring the Windows Time Service .....	46
6.17	Managing remote administration .....	46
6.17.1	Configuring with MDM .....	46
6.17.2	Configuring with group policy .....	47
6.17.3	Configuring with PowerShell.....	47
6.18	Managing Software Restriction Policies (SRP).....	47
6.18.1	Configuring with Software Restriction Policies .....	47
6.18.2	Configuring with AppLocker .....	48
6.19	Managing hibernation.....	49
6.19.1	Configuring with the Powercfg utility.....	49
6.20	Managing health attestation.....	49
6.20.1	Configuring with MDM .....	49

## Microsoft Windows 10 GP OS Administrative Guidance

6.20.2	Helper utility for health attestation logs .....	49
6.21	Managing audit policy.....	50
6.21.1	Scope of logging and auditing settings .....	50
6.21.2	Setting audit policy with Auditpol, Secpol, and Wevtutil.....	51
6.22	Developing Applications.....	53
7	Audit events .....	54
7.1	Audit events – GP OS protection profile .....	54
7.2	Audit events – WLAN client extended package.....	56
7.3	Events mapped to log details .....	58





## 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 Introduction

---

This administrative guide provides information for Windows 10 April 2018 Update and Windows Server version 1803, as required by the Common Criteria General Purpose Operating System (GP OS) protection profile. All Windows 10 and Windows Server 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 and Windows Server. IT Administrators must follow the guidance in this document to ensure a device matches the evaluated configuration.

### 3.1 What's new

The following list provides a summary of the substantive changes in since the last evaluation of Windows 10 and Windows Server against the Common Criteria GP OS protection profile.

- The administrative guide has been re-authored with a new template, simplified formatting, and additional contextual information.
- The scope of certification has grown to include the WLAN Client Extended Package and the administrative guide has been updated to match.


### 3.2 How this guide is organized

The sections in this administrative guide group information together categorically as follows:

- 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.
- 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 TechNet and other 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 Windows 10 and Windows Server 10 version 1803 GP OS Security Target and is available on the following sites:

- Microsoft publishes all Common Criteria evaluation documentation at <https://msdn.microsoft.com/en-us/library/dd229319.aspx>.
- 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:

- IT Administrator – a remote administrator using Mobile Device Management (MDM) or Group Policy Objects (GPO) to administer Windows.
- Local Administrator – a user account that is a member of the local Administrators group.
- Standard User – a user account that is not a member of the local Administrators group.

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 Mobile device management


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

The evaluation was performed both with devices enrolled in mobile 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 be used to administer devices running Windows 10 Home Edition, but not all CSPs can affect management functions on Windows 10 Home Edition. For each CSP referenced, this guide will identify which Windows editions it is available on. MDM may not be used to administer Windows Server editions.

The following articles provide general information on using MDM to administer Windows:

- 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>

 **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 mobile device management (MDM):

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

Policies may be configured by the IT Administrator using MDM and the Policy Configuration Service Provider. See the MDM solution documentation for detailed configuration actions. The following article details the Policy CSP and its functions:

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


 **Note:** Some of the Policy CSP functions are not available on Windows 10 Home Edition. The article above provides a compatibility chart for each of the Policy CSP functions. For a reference on CSPs beyond the Policy CSP, see the following article:

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

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

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

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 scripts:

<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:

- <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\FipsAlgorithm
Policy -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 1803 (April 2018 Update)
- Microsoft Windows 10 Pro Edition version 1803 (April 2018 Update)
- Microsoft Windows 10 Enterprise Edition version 1803 (April 2018 Update)
- Microsoft Windows Server Standard Core, version 1803
- Microsoft Windows Server Datacenter Core, version 1803

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**

Home, Pro, Enterprise, Server Standard, Server Datacenter

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

- Microsoft Surface Book 2
- Microsoft Surface Pro LTE
- Microsoft Surface Laptop
- Microsoft Surface Go
- Dell Latitude 5290
- Dell Latitude 12 Rugged Tablet
- Dell PowerEdge R740<sup>1</sup> (representing the 14<sup>th</sup> generation of PowerEdge servers.)
- Microsoft Windows Server Hyper-V
- Microsoft Windows Server 2016 Hyper-V

## 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.

---

<sup>1</sup> The Dell PowerEdge R440, R540, R640, R740XD, T440, T640, R940, R940xa, R840, M640, M640p, FC640, MX740c, MX840c, C6420, C4140, XR2, and Dell Precision 7920 Rack all use the same processor, memory, chipset, and TPM and could be considered equivalent.

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 topic includes procedures to download installation media as an ISO file for installation, create bootable media using the ISO file, and install the operating system:  
<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 mobile device management in order to receive MDM policies. For Windows Server IT administration is joining the device to a Windows domain in order to received 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 July 30, 2018 installed. See section 1 of the Security Target for related information. The current list of updates for this version of Windows, including those available as of July 30, 2018, is available at <https://support.microsoft.com/en-us/help/4099479/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 cryptography mode

To match the evaluated configuration, Windows cryptography must be placed into the FIPS 140 mode. Choosing this mode ensures Windows uses FIPS 140 compliant cryptographic algorithms, including 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 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, Local 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>	Standard User
<b>Windows Editions</b>	Home

To set FIPS mode for Windows Home edition, 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 6.3.6, [Generating X.509 certificates with templates](#), for implementation guidance.

## 5.2.7 Device access

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

- Complex passwords must be required. See section 6.7, [Managing passwords and password policy](#), for implementation guidance.
- Session locking must be enabled. See section 6.10, [Managing screen lock and session timeout](#), for implementation guidance.
- Hibernation must be disabled. See section 6.19, [Managing Hibernation](#), 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.
- Unprotected keys are not stored in non-volatile memory.
- Windows automatically generates asymmetric RSA keys using methods that meet FIPS-PUB 186-4 Appendix B.3, no configuration is necessary.
- Windows automatically generates asymmetric ECC keys using methods that meet FIPS-PUB 186-4 Appendix B.4, no configuration is necessary.
- Windows automatically implements RSA-based key establishment schemes that meet SP800-56B, no configuration is necessary.
- Windows automatically implements elliptic curve-based key establishment schemes that meet SP800-56A, no configuration is necessary.
- Windows automatically generates random bits according to SP-800-90A, no configuration is necessary.

## 6.2 Managing X.509 certificates

### 6.2.1 Client certificates and Certificate Authorities

An IT Administrator may specify the list of Certificate Authorities (CAs) from which the device will accept X.509 certificates and WLAN authentication server certificates. The following article provides an overview of certificate management in Windows, including requesting certificates, enrolling, and managing certificate path validation:

- Manage Certificates: <http://technet.microsoft.com/en-us/library/cc771377.aspx>

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: <http://technet.microsoft.com/library/cc732443.aspx>

#### 6.2.1.1 Configuring with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Home, 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>

#### 6.2.1.2 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:

- 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>

## 6.2.2 Root certificates

Windows is preloaded with root certificates for several Certification Authorities (CAs). The following article provides an overview of managing trusted root certificates for a local computer or a domain, including how to add certificates to the store:

- Manage Trusted Root Certificates: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754841\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc754841(v=ws.11))

### 6.2.2.1 Configuring with MDM

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

The following TechNet topic also describes how to manage trusted roots with the Group Policy Editor or Local Security Policy Editor:

- Manage Trusted Root Certificates: <http://technet.microsoft.com/en-us/library/cc754841.aspx>

The following TechNet topic describes how to delete a certificate with the Group Policy Editor or Local Security Policy Editor:

- Delete a Certificate: <http://technet.microsoft.com/en-us/library/cc772354.aspx>

### 6.2.2.3 Configuring with PowerShell

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

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

PowerShell provides multiple cmdlets to manage certificates, as described below.

The remove-item PowerShell cmdlet may be used to delete certificates and wipe the private keys associated with the certificate. The following article describes how to use the cmdlet:

- [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-powershell-1.0/ee176938\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-powershell-1.0/ee176938(v=technet.10))

The import-pfxcertificate PowerShell cmdlet may be used to import a certificate and private key from a PFX file. The following article describes how to use the cmdlet:

- <https://docs.microsoft.com/en-us/powershell/module/pkiclient/import-certificate?view=win10-ps>

The export-pfxcertificate may be used to export a certificate and private key to a PFX file. The following article describes how to use the cmdlet:

- <https://docs.microsoft.com/en-us/powershell/module/pkiclient/export-pfxcertificate?view=win10-ps>

### 6.2.3 Certificate name comparison

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

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

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.

#### 6.2.4.1 Configuring certificate validation with PowerShell

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

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

The administrator configures certificate validation using the Set-NetFirewallSetting PowerShell cmdlet as described in the following TechNet topic:

- Set-NetFirewallSetting: <http://technet.microsoft.com/en-us/library/jj554878.aspx>

#### 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 in the "Smart Card or Other Certificate Properties" and "Configure Certificate Selection" screens as described in the following article:

- Extensible Authentication Protocol (EAP) Settings for Network Access (see Smart Card or other Certificate Properties configuration items): <https://technet.microsoft.com/en-us/library/hh945104.aspx>

#### 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:  
<http://blogs.msdn.com/b/ieinternals/archive/2011/04/07/enabling-certificate-revocation-check-failure-warnings-in-internet-explorer.aspx>

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)

### 6.3.1 Available ciphersuites

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

<b>Ciphersuites listed in the Security Target</b>	<b>Setting name for the ciphersuite in Windows</b>
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_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
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
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256



Ciphersuites listed in the Security Target	Setting name for the ciphersuite in Windows
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384

See the following topic for additional information on TLS ciphersuites, see TLS Ciphersuites in Windows 10 1803:

- <https://docs.microsoft.com/en-us/windows/desktop/SecAuthN/tls-cipher-suites-in-windows-10-v1803>

### 6.3.2 Available TLS-EAP ciphersuites

The TLS-EAP 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_128_CBC_SHA256 as defined in RFC 5246	TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246	TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246	TLS_RSA_WITH_AES_256_CBC_SHA256
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 cipher suite 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#ryptography-tlsciphersuites>

### 6.3.4 Configuring with group policy

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

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)
- How to restrict the use of certain cryptographic algorithms and protocols in Schannel.dll: <https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc>

 **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.

### 6.3.5 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:

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

### 6.3.6 Generating X.509 certificates with templates

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:

- Managing Certificate Templates: <https://technet.microsoft.com/en-us/library/cc772457.aspx>
- 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_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	Provider Category = Key Storage Provider  Algorithm Name = RSA

Ciphersuites (per Security Target)	Selections in the certificate template
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289	Provider Category = Key Storage Provider  Algorithm Name = ECDSA_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 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
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 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_P521

### 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 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.

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

<b>Role</b>	Standard User,
<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)

### 6.4.2 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>

### 6.4.3 Configuring Wi-Fi access with MDM

<b>Role</b>	IT Administrator
<b>Windows Editions</b>	Home, 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 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>

#### 6.4.4 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>

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

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

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>

#### 6.4.6 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>

### 6.4.7 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.

### 6.4.8 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
- 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

## 6.5 Managing personal hotspots

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

### 6.5.1 Configuring with MDM

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

Sharing a personal hotspot may be enabled/disabled 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 personal hotspots:



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

## 6.5.2 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

## 6.5.3 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**

## 6.6 Managing Bluetooth

This section provides various configuration instructions for managing Bluetooth. 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.

### 6.6.1 Configuring Bluetooth adapters with MDM

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

The Bluetooth radio may also 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>.

### 6.6.2 Enabling or disabling Bluetooth adapters with the Windows UI

<b>Role</b>	Standard User
<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

### 6.6.3 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 Managing passwords and password policy

### 6.7.1 Configuring with MDM

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

Password policy may be configured by the IT Administrator using MDM. See the MDM solution documentation for detailed actions. The DeviceLock policies, part of the 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 the documentation:

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

### 6.7.2 Configuring with group policy

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

The Group Policy Editor or Local Security Policy Editor may also be used to set password security policies on Windows 10 Enterprise, Windows 10 Pro,. The following article provides an overview of password security policies and links to information for each security policy setting:

- Password Policy: [https://technet.microsoft.com/en-us/library/hh994572\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/hh994572(v=ws.10).aspx)

The Administrator may disable unauthenticated logon by configuring user accounts to have a password. The OOB requires user accounts to be created with a password.

### 6.7.3 Configuring with net accounts utility

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

The following article explains the net accounts command line utility for standalone computers, which provides command-line options for managing password and account lockout policy:

- 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.

## 6.8 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 topic and its sub-topics:

- 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>

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

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

## 6.9 Managing Windows Hello

### 6.9.1 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

### 6.9.2 Configuring PIN authentication with group policy

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

To enable using a PIN in place of passwords on domain-joined devices, the following security policy must be enabled using the Group Policy Editor:


- Administrative Templates\System\Logon\Turn on convenience PIN sign-in.

### 6.9.3 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

 **Note:** The PIN sign-in options user interface is not displayed when the device is logged on remotely via Remote Desktop Protocol or when it is hosted in a Hyper-V virtual machine in Enhanced Session mode.

## 6.10 Managing screen lock and session timeout

### 6.10.1 Configuring with MDM

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

Screen lock and session timeout be configured by the IT Administrator using MDM. See the MDM solution documentation for detailed actions. The DeviceLock policies, part of the Policy CSP, provide a variety of management functions for screen lock and session timeout. 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 the documentation:

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

### 6.10.2 Configuring with group policy

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

Screen lock and session timeout can both be configured by a Windows security policy. The relevant policies are:

- For local session locking, use the security policy **Interactive logon: Machine inactivity limit**. The following article provides details in the section titled **New and changed functionality**: Security Policy Settings Overview: <http://technet.microsoft.com/en-us/library/2fdccb11-8037-45b1-9015-665393268e36>
- For remote session locking, use the security policy **Set time limit for active but idle Remote Desktop Services session**. The following article includes details: Session Time Limits: <https://technet.microsoft.com/en-us/library/ee791741.aspx>

### 6.10.3 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>

### 6.10.4 Configuring with the Windows user interface

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

There are multiple user-configurable settings in Windows that enable control over different aspects of locking notifications while in a locked state.

To configure screen lock timeout, use the Settings app:

- Go to **Settings**
- Navigate to **System > Power & sleep > Additional power settings > Change when the computer sleeps**
- Choose a timeout duration

The user can set the scope of notifications shown on screen in a locked state via the Settings app:

- Go to **Settings**
- Navigate to **System > Notifications & actions**

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

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

## 6.11 Managing the logon banner

### 6.11.1 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>.

### 6.11.2 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:

- 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>

### 6.11.3 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

## 6.12 Managing USB

### 6.12.1 Configuring with the Windows UI

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

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

### 6.12.2 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>

### 6.12.3 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 topic:

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

## 6.13 Managing updates

The following article provides an overview of Windows Update and matching FAQ list:

- 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 than the default Microsoft Update. Configuring WSUS is outside the scope of this document.

### 6.13.1 Configuring using MDM

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

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>

### 6.13.2 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>

### 6.13.3 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>

### 6.13.4 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.

### 6.13.5 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 topics:

- 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)

### 6.13.6 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 Managing the firewall

### 6.14.1 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>

## 6.15 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 choosing a Management Server.

### 6.15.1 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>

## 6.16 Managing date and time

### 6.16.1 Configuring with PowerShell

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

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>

## 6.16.2 Configuring the Windows Time Service

<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>

## 6.17 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>

### 6.17.1 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. See the

MDM solution documentation for detailed configuration actions. The following article describes the correct function in the Policy CSP to use:

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

### 6.17.2 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>

### 6.17.3 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 link provides information about PowerShell Remoting Security Considerations:

- <https://docs.microsoft.com/en-US/powershell/scripting/setup/winrmsecurity?view=powershell-6>

## 6.18 Managing Software Restriction Policies (SRP)

### 6.18.1 Configuring with Software Restriction Policies

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

Device Guard is used to manage Software Restriction Policies. See the link below for information on Device Guard:

- Device Guard: Windows Defender Application Control and virtualization-based protection of code integrity: <https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows-defender-application-control>

The following sample PowerShell script demonstrates a Device Guard policy to deny executing the Microsoft Edge browser application:

```
# By default no binaries are allowed to run so we need to allow most windows binaries
to run first.
# This will not allow unsigned binaries to execute.
# Add the set of signed binaries in "Program Files" and "Windows" folders and allow
them to execute.
New-CIPolicy -Level PcaCertificate -UserPES -ScanPath 'C:\Program Files' -FilePath
allowProgramFiles.xml
New-CIPolicy -Level PcaCertificate -UserPES -ScanPath C:\Windows -FilePath
allowWindows.xml

# deny the Microsoft Edge app (which would otherwise be whitelisted by the above rule)
New-CIPolicy -Level FileName -UserPES -Deny -ScanPath
C:\Windows\SystemApps\Microsoft.MicrosoftEdge_8wekyb3d8bbwe -FilePath denyEdge.xml

# enforce the rules
Set-RuleOption -Delete 3 -FilePath allowProgramFiles.xml
Set-RuleOption -Delete 3 -FilePath allowWindows.xml
Set-RuleOption -Delete 3 -FilePath denyEdge.xml

#merge the three policy files and deploy the policy
Merge-CIPolicy -PolicyPaths
'.\denyEdge.xml', '.\allowWindows.xml', 'allowProgramFiles.xml' -OutputFilePath
mergedPolicy.xml
convertFrom-CIPolicy mergedPolicy.xml mergedPolicy.bin
copy mergedPolicy.bin c:\windows\system32\codeintegrity\sipolicy.p7b
```


## 6.18.2 Configuring with AppLocker

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

AppLocker may also be used to manage Software Restriction Policies. Depending on the environment and business requirements, administrators may choose to use both Device Guard and AppLocker. See the topics below for information on AppLocker and on deciding whether to use AppLocker, Device Guard, or both:

- AppLocker Overview: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview>
- Windows Defender Device Guard with AppLocker: <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-device-guard-and-applocker>



 **Note:** AppLocker is only supported in Windows 10 Enterprise edition. All editions, except Enterprise, should use Device Guard to manage Software Restriction Policies

## 6.19 Managing hibernation

### 6.19.1 Configuring with the Powercfg utility

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

The following article describes how to manage power configuration, including disabling the hibernate function:

- Powercfg Command-Line Options: <https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/powercfg-command-line-options>

## 6.20 Managing health attestation

### 6.20.1 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. See the MDM solution documentation for detailed configuration actions. The following article provides details on the correct CSP to use to manage health attestation policies with MDM:

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

### 6.20.2 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>

## 6.21 Managing audit policy

<b>Role</b>	All
<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.

### 6.21.1 Scope of logging and auditing settings

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)

The following article provides more information on security audit policies, including planning and deploying the policies:

- Advanced security audit policies: <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing>

## 6.21.2 Setting audit policy with Auditpol, Secpol, and Wevtutil

The Auditpol command displays information about and performs functions to manipulate audit policies. 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/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc731451\(v%3dws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc731451(v%3dws.11))

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/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc755264\(v%3dws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/cc755264(v%3dws.11))

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
```

- 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
```

The Local Security Policy (secpol.msc) utility is used as an alternative to the auditpol utility for managing Security audits. The following article describes how to use the Local Security Policy utility:

- Administer security policy settings: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj966254\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj966254(v=ws.11))

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
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 topic describes System Access Control Lists in general:

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

Wevtutil is a system utility that performs many of the management functions related to system and audit logons 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>

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 topic:

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

## 6.22 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>

## 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.

<b>Description</b>	<b>Context: Event ID (Detail)</b> <b>Note – all events are in the Security log.</b>
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>

## Microsoft Windows 10 GP OS Administrative Guidance

Description	Context: Event ID (Detail) Note – <i>all</i> events are in the Security log.
	Failure: <b>4674</b>
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 and unlock 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>

Description	Context: Event ID (Detail) Note – <i>all</i> events are in the Security log.
Program initiations (Success/Failure e.g. due to software restriction policy)	Success: <b>3038</b> (Device Guard), <b>8020</b> (AppLocker) Failure: <b>3077</b> (Device Guard) , <b>8022</b> (AppLocker)
Startup and shutdown of the RichOS, IE 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	<u>Log Name</u> : Event ID (Detail)
FAU_GEN.1/WLAN	None.		





## Microsoft Windows 10 GP OS Administrative Guidance

<b>Requirement</b>	<b>Auditable Events</b>	<b>Additional Audit Record Contents</b>	<b><u>Log Name:</u> Event ID (Detail)</b>
FCS_CKM.1/WLAN	None.		
FCS_CKM.2/WLAN	None.		
FCS_CKM_EXT.4	None.		
FCS_TLSC_EXT.1/WLAN	Failure to establish an EAP-TLS session.	Reason for failure	<u>System:</u> <b>36888</b> <u>Microsoft-Windows-CAPI2/Operational:</u> <b>11, 30</b>
	Establishment/termination of an EAP-TLS session.	Non-TOE endpoint of connection.	<u>System:</u> <b>36880</b> (Establishment) <u>Microsoft-Windows-SChannel-Events/Perf:</u> <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>detected integrity violation</i> ].	[Selection: <i>The TSF binary file that caused the integrity violation</i> ].	<u>System:</u> <b>20</b>

Requirement	Auditable Events	Additional Audit Record Contents	<u>Log Name: Event ID (Detail)</u>
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).	<u>Microsoft-Windows-WLAN-AutoConfig/Operational log event:</u> <b>8001</b> (successful WLAN connection) <b>8002</b> (WLAN connection failure) <b>8003</b> (successful WLAN disconnection) <b>8004</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 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.

Microsoft Windows 10 GP OS Administrative Guidance

Event ID	Location in Log	Message	Fields
2		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 update could not be installed because ... "The data is invalid"	<b>Windows Logs-&gt;Setup</b>
11	<b>Microsoft-Windows-CAPI2/Operational</b>	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	<b>Windows Logs -&gt; System</b>	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>

Microsoft Windows 10 GP OS Administrative Guidance

Event ID	Location in Log	Message	Fields
30	Microsoft-Windows-CAPI2/Operational	Verify Chain Policy	<p><b>System-&gt;TimeCreated[SystemTime]:</b> &lt;Date and time of event&gt;</p> <p><b>System-&gt;Provider[Name]:</b> &lt;Type of event&gt;</p> <p><b>System-&gt;Level:</b> &lt;Outcome as Success or Failure&gt;</p> <p><b>System-&gt;Security[UserID]:</b> &lt;Subject identity&gt;</p> <p><b>UserData-&gt;CertVerifyCertificateChainPolicy-&gt;Certificate:</b> &lt;Issuer Name and Subject Name of certificate&gt;</p>
1100		The event logging service has shut down	<b>Windows Logs-&gt;Setup</b>
1793	Microsoft-Windows-SChannel-Events/Perf	A TLS Security Context handle is being deleted	<p><b>System-&gt;TimeCreated[SystemTime]:</b> &lt;Date and time of event&gt;</p> <p><b>System-&gt;Provider[Name]:</b> &lt;type of event&gt;</p> <p><b>System-&gt; Security[UserID]:</b> &lt;subject identifier &gt;</p> <p><b>System-&gt;Level:</b> &lt;Outcome as Success or Failure&gt;</p> <p><b>EventData-&gt;ContextHandle:</b> &lt;non-TOE endpoint&gt;</p>
3004		Windows is unable to verify the image integrity of the file <pathname> because the file hash could not be found on the system.	<p><b>Windows Logs-&gt;Security</b></p> <p>Subcategory: Security State Change</p>



## Microsoft Windows 10 GP OS Administrative Guidance

Event ID	Location in Log	Message	Fields
3038	<b>Application and Services Logs-&gt;Microsoft-&gt;Windows-&gt;CodeIntegrity-&gt;Verbose</b>	Code Integrity started validating image header of <kernel module pathname> file	<b>Application and Services Logs-&gt;Microsoft-&gt;Windows-&gt;CodeIntegrity-&gt;Operational</b>
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.	<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>
4624	<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>

Microsoft Windows 10 GP OS Administrative Guidance

Event ID	Location in Log	Message	Fields
4625	<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>
4656	<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>
4670	<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>
4673	<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>

Microsoft Windows 10 GP OS Administrative Guidance

Event ID	Location in Log	Message	Fields
4674	<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>
4720	<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>
4725	<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>
4726	<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>

Microsoft Windows 10 GP OS Administrative Guidance

Event ID	Location in Log	Message	Fields
4731	<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>
4732	<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>
4733	<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>
4734	<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>





## Microsoft Windows 10 GP OS Administrative Guidance

Event ID	Location in Log	Message	Fields
4735	<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>
4738	<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>
4740	<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>
4767	<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

Event ID	Location in Log	Message	Fields
8001	<b>Microsoft-Windows-WLAN-AutoConfig/Operational</b>	WLAN AutoConfig service has successfully connected to a wireless network	<p><b>System-&gt;TimeCreated[SystemTime]:</b> &lt;Date and time of event&gt;</p> <p><b>System-&gt;Provider[Name]:</b> &lt;Type of event&gt;</p> <p><b>System-&gt;Level:</b> &lt;Outcome as Success or Failure&gt;</p> <p><b>System-&gt;Security[UserID]:</b> &lt;Subject identity&gt;</p> <p><b>EventData-&gt;PHYType, AuthenticationAlgorithm:</b> &lt;Trusted channel protocol&gt;</p> <p><b>EventData-&gt;SSID:</b> &lt;Non-TOE endpoint of connection&gt;</p>
8002	<b>Microsoft-Windows-WLAN-AutoConfig/Operational</b>	WLAN AutoConfig service failed to connect to a wireless network	<p><b>System-&gt;TimeCreated[SystemTime]:</b> &lt;Date and time of event&gt;</p> <p><b>System-&gt;Provider[Name]:</b> &lt;Type of event&gt;</p> <p><b>System-&gt;Level:</b> &lt;Outcome as Success or Failure&gt;</p> <p><b>System-&gt;Security[UserID]:</b> &lt;Subject identity&gt;</p> <p><b>EventData-&gt;PHYType, AuthenticationAlgorithm:</b> &lt;Trusted channel protocol&gt;</p> <p><b>EventData-&gt;SSID:</b> &lt;Non-TOE endpoint of connection&gt;</p>

Microsoft Windows 10 GP OS Administrative Guidance

Event ID	Location in Log	Message	Fields
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>
8004	<b>Microsoft-Windows-WLAN-AutoConfig/Operational</b>	Wireless network is blocked due to connection failure.	<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;FailureReason:</b> <Failure condition> <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>

Microsoft Windows 10 GP OS Administrative Guidance

Event ID	Location in Log	Message	Fields
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>
11005	<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>
11006	<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>

Microsoft Windows 10 GP OS Administrative Guidance

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

Microsoft Windows 10 GP OS Administrative Guidance

Event ID	Location in Log	Message	Fields																												
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> <table border="0"> <tr><td>10</td><td>Unexpected message</td></tr> <tr><td>20</td><td>Bad record MAC</td></tr> <tr><td>22</td><td>Record overflow</td></tr> <tr><td>30</td><td>Decompression fail</td></tr> <tr><td>40</td><td>Handshake failure</td></tr> <tr><td>47</td><td>Illegal parameter</td></tr> <tr><td>48</td><td>Unknown CA</td></tr> <tr><td>49</td><td>Access denied</td></tr> <tr><td>50</td><td>Decode error</td></tr> <tr><td>51</td><td>Decrypt error</td></tr> <tr><td>70</td><td>Protocol version</td></tr> <tr><td>71</td><td>Insufficient security</td></tr> <tr><td>80</td><td>Internal error</td></tr> <tr><td>110</td><td>Unsupported extension</td></tr> </table>	10	Unexpected message	20	Bad record MAC	22	Record overflow	30	Decompression fail	40	Handshake failure	47	Illegal parameter	48	Unknown CA	49	Access denied	50	Decode error	51	Decrypt error	70	Protocol version	71	Insufficient security	80	Internal error	110	Unsupported extension
10	Unexpected message																														
20	Bad record MAC																														
22	Record overflow																														
30	Decompression fail																														
40	Handshake failure																														
47	Illegal parameter																														
48	Unknown CA																														
49	Access denied																														
50	Decode error																														
51	Decrypt error																														
70	Protocol version																														
71	Insufficient security																														
80	Internal error																														
110	Unsupported extension																														

