Operational and Administrative Guidance

Microsoft Windows 10 and Windows Server 2019

Common Criteria Evaluation for Microsoft Windows 10 and Windows Server 2019 Version 1809 (October 2018 Update)

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.

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.

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

Version	Date	Description
1.0	March 20, 2018	Administrative Guide for Windows 10 and Windows Server Fall Creators Update (1709)
2.0	October 11, 2018	Administrative Guide for Windows 10 and Windows Server April 2018 Update (1803)
3.0	June 18, 2019	Administrative Guide for Windows 10 and Windows Server 2019, Version 1809 (October 2018 Update)

3 Introduction

This administrative guide provides information for Windows 10 version 1809 (October 2018 Update) and Windows Server 2019, , as required by the Common Criteria General Purpose Operating System (GP OS) protection profile. All Windows 10 and Windows Server 2019 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.

- This administrative guide now includes the Configuration Annex Release 1 for PP GPOS version 4.2. See section 8, Configuration Annex, for the list of Configuration Actions.

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.
- Section 8, Configuration Annex, lists the Configuration Actions that are a part of the Configuration Annex Release 1 for PP GPOS version 4.2 and references the relevant guidance in other sections of this administrative guide.

3.3 Links to other resources

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

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

3.4 Security Target document

The Common Criteria evaluation requires a Security Target document that outlines the evaluation scope, which this guide may refer to. The correct matching Security Target for this administrative guide is the Microsoft Windows 10, Windows Server 2019 (October 2018 Update) Security Target and is available on the following sites:

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

3.5 Guidance specific to user roles

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

- IT Administrator – a remote administrator using Modern 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:

Role	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)

3.6 Modern device management

Role	IT Administrator
Windows Editions	Pro, Enterprise

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

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

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

- 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 modern device management (MDM):

Role	IT Administrator
Windows Editions	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.

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):

Role	IT Administrator, Local Administrator
Windows Editions	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:

Role	IT Administrator, Local Administrator
Windows Editions	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 (October 2018 Update) (32-bit and 64-bit versions)

- Microsoft Windows 10 Pro edition (October 2018 Update) (64-bit version)
- Microsoft Windows 10 Enterprise edition (October 2018 Update) (64-bit version)
- Microsoft Windows Server 2019 Standard edition, version 1809
- Microsoft Windows Server 2019 Datacenter edition, version 1809

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 Go
- Microsoft Surface Book 2
- Microsoft Surface Pro LTE
- Microsoft Surface Laptop
- Microsoft Windows Server 2019 Hyper-V
- Microsoft Windows Server 2016 Hyper-V
- Dell Latitude 5290
- Dell Latitude 12 Rugged Tablet
- Dell PowerEdge R740
- Samsung Galaxy Book 10.6”
- Samsung Galaxy Book 12”
- HP Elite x2 1013 G3 Tablet
- HP EliteBook x360 1030 G2

5 Evaluated configuration

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

5.1 Installing the operating system

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

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

- For all editions except Enterprise, the following 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 modern device management (MDM) 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 November 30, 2018 installed. See section 1 of the Security Target for related information. The following topic provides a current list of updates for this version of Windows, including those available as of November 30, 2018:

- Windows 10 and Windows Server 2019 update history: https://support.microsoft.com/en-us/help/4464619

5.2.4 Mode of operation

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

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

5.2.5 FIPS 140 Approved mode

To match the evaluated configuration, Windows cryptography must be placed into the FIPS 140 Approved mode.

5.2.5.1 Configuring with MDM

Role	IT Administrator
Windows Editions	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

Role	IT Administrator, Local Administrator
Windows Editions	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
Local Policies\Security Options\System cryptography: 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

Role	Standard User
Windows Editions	All

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

Registry Node	Setting
HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\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.
- Windows generates asymmetric RSA keys using methods that meet FIPS-PUB 186-4 Appendix B.3, no configuration is necessary.
- Windows generates asymmetric ECC keys using methods that meet FIPS-PUB 186-4 Appendix B.4, no configuration is necessary.
- Windows performs RSA-based key establishment that meet NIST SP 800-56B, no configuration is necessary.
- Windows performs elliptic curve-based key schemes that meet NIST SP 800-56A, no configuration is necessary.
- Windows generates random numbers according to NIST SP 800-90A, no configuration is necessary.
- Unprotected keys are not stored in non-volatile memory.

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

Role	IT Administrator
Windows Editions	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

Role	Standard User
Windows Editions	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 Trusted root certificates

Windows is preloaded with trusted 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)

6.2.2.1 Configuring with MDM

Role	IT Administrator
Windows Editions	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

Role	IT Administrator, Local Administrator
Windows Editions	Pro, Enterprise, Server Standard, Server Datacenter

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

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

6.2.2.3 Configuring with PowerShell

Role	Standard User, Local Administrator
Windows Editions	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)

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

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

Role	Standard User, Local Administrator
Windows Editions	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

Role	Standard User, Local Administrator
Windows Editions	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

Role	Standard User, Local Administrator
Windows Editions	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 TLS ciphersuites

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

Ciphersuites listed in the Security Target	Setting name for the ciphersuite in Windows
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246	TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246	TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246	TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_ SHA384 as defined in RFC 5288	TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_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_CBC_SHA384 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

See the following topic for additional information on TLS ciphersuites:

- TLS Ciphersuites in Windows 10 1809: https://docs.microsoft.com/en-us/windows/desktop/SecAuthN/tls-cipher-suites-in-windows-10-v1809

6.3.2 Available EAP-TLS ciphersuites

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

Ciphersuites listed in the Security Target	Setting name for the ciphersuite in Windows
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246	TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_ SHA as defined in RFC 5246	TLS_RSA_WITH_AES_256_CBC_ SHA
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246	TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246	TLS_RSA_WITH_AES_256_CBC_ SHA256
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

Role	IT Administrator
Windows Editions	Pro, Enterprise

TLS ciphersuite priority and restricting use of certain cryptographic algorithms may be

configured by the IT Administrator using MDM. See the MDM solution documentation for detailed configuration actions. The following article describes the CSP used with MDM to set policy for TLS ciphersuites:

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

6.3.4 Configuring with PowerShell

Role	Standard User, Local Administrator
Windows Editions	All

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

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

- Enable-TlsCipherSuite
- Disable-TlsCipherSuite
- Enable-TlsEccCurve
- Disable-TlsEccCurve

6.3.5 Configuring with group policy

Role	IT Administrator, Local Administrator
Windows Editions	Pro, Enterprise, Server Standard, Server Datacenter

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

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

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

6.3.6 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:

- Configure the Server Certificate Template: https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/configure-the-server-certificate-template
- 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)
- 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_GCM_ SHA384 as defined in RFC 5288 TLS_ECDHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_CBC_ SHA384 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_GCM_ SHA384 as defined in RFC 5289	Provider Category = Key Storage Provider Algorithm Name = RSA

Ciphersuites (per Security Target)	Selections in the certificate template
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_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_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

Role	Standard User, Local Administrator
Windows Editions	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

Role	Standard User
Windows Editions	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

Role	Standard User,
Windows Editions	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

6.4.2 Enabling or disabling network connections with PowerShell

Role	Standard User, Local Administrator
Windows Editions	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

Role	IT Administrator
Windows Editions	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

Role	Standard User

Windows Editions	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

Role	IT Administrator
Windows Editions	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

Role	IT Administrator, Local Administrator
Windows Editions	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

Role	Standard User

Windows Editions	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

Role	Standard User
Windows Editions	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

Role	IT Administrator
Windows Editions	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

Role	IT Administrator, Local Administrator,
Windows Editions	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

Role	Standard User
Windows Editions	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

Role	IT Administrator
Windows Editions	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

Role	Standard User
Windows Editions	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

Role	Standard User, Local Administrator
Windows Editions	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

Role	IT Administrator
Windows Editions	Pro, Enterprise

Password policy may be configured using MDM. The DeviceLock policies, part of the larger

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

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

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

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

6.7.2 Configuring with group policy

Role	IT Administrator, Local Administrator
Windows Editions	Pro, Enterprise, Server Standard, Server Datacenter

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

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

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

- Disabling the Guest account: Use the setting **Accounts: Guest account status** under **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options**. For more information, see: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-guest-account-status.
- Specifying password length: Use the setting **Minimum password length** under **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**. For more information, see: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/minimum-password-length.
- Specifying password complexity: Use the setting **Passwords must meet complexity requirements** under **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**. For more information, see: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements
- Specifying the maximum number of authentication failures: Use the setting **Account lockout threshold** under **Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy** to set the maximum number of failures. For more information, see: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold.
- Specifying the duration within which to enforce the maximum number of authentication failures: Use the setting **Account lockout duration** under **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**. For more information, see: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-duration.

6.7.3 Configuring with net.exe accounts utility

Role	Local Administrator
Windows Editions	All

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

- Forcing user logoff after a time interval
- Minimum and maximum password age (days)
- Minimum password length
- Length of password history maintained
- Lockout threshold

- Lockout duration (minutes)
- Lockout observation window (minutes)

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

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

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

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

6.8 Managing smart card logon

Role	IT Administrator, Local Administrator
Windows Editions	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

Role	Standard User
Windows Editions	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 Windows Hello for Business with group policy or MDM

Role	IT Administrator, Local Administrator
Windows Editions	Pro, Enterprise

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

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

6.9.3 Configuring PIN authentication with the Windows UI

Role	Standard User
Windows Editions	Home, Pro, Enterprise

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

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

6.10 Managing screen lock and session timeout

6.10.1 Configuring with MDM

Role	IT Administrator
Windows Editions	Pro, Enterprise

The DeviceLock policies, part of the larger Policy CSP, provide 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 an overview of DeviceLock and a listing of all functions available:

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

Among these functions, the following policy can be used to enable screen lock and set the lock timeout period. The article link provides detailed information on the policy function and how to implement it.

- Configuring screen lock: Use the policy **DeviceLock/MaxInactivityTimeDeviceLock**. For more information, see: https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-devicelock#devicelock-maxinactivitytimedevicelock.

6.10.2 Configuring with group policy

Role	IT Administrator, Local Administrator
Windows Editions	Pro, Enterprise, Server Standard, Server Datacenter

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

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

6.10.3 Configuring with the Windows registry

Role	Local Administrator, Standard User
Windows Editions	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

Role	Standard User
Windows Editions	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

Role	IT Administrator
Windows Editions	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-interactivelogon-displayuserinformationwhenthesessionislocked.

6.11.2 Configuring with group policy

Role	IT Administrator, Local Administrator
Windows Editions	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

Role	Local Administrator
Windows Editions	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

Role	Standard User
Windows Editions	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

Role	Standard User, Local Administrator
Windows Editions	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

Role	Local Administrator
Windows Editions	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 the default Microsoft Update. Configuring WSUS is outside the scope of this document.

6.13.1 Configuring using MDM

Role	IT Administrator
Windows Editions	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

Role	IT Administrator, Local Administrator
Windows Editions	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

Role	Local Administrator
Windows Editions	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

Role	Standard User
Windows Editions	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

Role	Local Administrator

Windows Editions	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

Role	Standard User
Windows Editions	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 diagnostic data

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

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

6.14.1 Configuring with group policy

Role	IT Administrator, Local Administrator
Windows Editions	Pro, Enterprise, Server Standard, Server Datacenter

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

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

6.14.2 Configuring with MDM

Role	IT Administrator
Windows Editions	Pro, Enterprise

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

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

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

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

6.14.3 Configuring with the Windows UI

Role	Standard User, Local Administrator
Windows Editions	Home

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

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

6.15 Managing the firewall

6.15.1 Configuring with PowerShell

Role	Standard User, Local Administrator
Windows Editions	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

6.16 Managing domains

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

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

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

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

6.16.1 Configuring with PowerShell

Role	Standard User, Local Administrator
Windows Editions	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

6.17Managing date and time

6.17.1 Configuring with PowerShell

Role	Standard User, Local Administrator
Windows Editions	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

6.17.2 Configuring the Windows Time Service

Role	All
Windows Editions	All

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

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

6.18 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

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

6.18.1 Configuring with MDM

Role	IT Administrator
Windows Editions	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

6.18.2 Configuring with group policy

Role	IT Administrator, Local Administrator
Windows Editions	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

6.18.3 Configuring with PowerShell

Role	Standard User, Local Administrator
Windows Editions	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

6.19 Managing Software Restriction Policies

6.19.1 Configuring with Windows Defender Application Control

Role	IT Administrator, Local Administrator
Windows Editions	All

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

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

6.19.2 Configuring with AppLocker

Role	IT Administrator, Local Administrator
Windows Editions	Enterprise

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

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

- AppLocker Overview, Design Guide, and Deployment Guide: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview

6.20 Managing hibernation

6.20.1 Configuring with the Powercfg utility

Role	Local Administrator
Windows Editions	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

6.21 Managing health attestation

6.21.1 Configuring with MDM

Role	IT Administrator
Windows Editions	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

6.21.2 Helper utility for health attestation logs

Role	Local Administrator
Windows Editions	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

6.22 Managing audit policy

Role	IT Administrator, Local Administrator
Windows Editions	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.

For background on configuring audit policies in Windows, see these articles:

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

6.22.1 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)

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)

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)

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

6.22.2 Configuring System Access Control Lists for audited objects

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

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

6.23 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.

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

Description	**Context: Event ID (Detail)** **Note – *all* events are in the Security log.**
File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions)	**4656**
User and Group management events (Successful and unsuccessful add, delete, modify, disable)	add user: **4720** add user to group: **4732** delete user: **4726** delete user from group: **4733** add group: **4731** delete group: **4734** modify group: **4735** modify user account: **4738** disable user: **4725**
Lock and unlock a user account	Lock: **4740** Unlock: **4767**
Audit and log data access events (Success/Failure)	Success, Failure: **4673**
Cryptographic verification of software (Success/Failure)	Failure: **3** Success: **2**
Program initiations (Success/Failure e.g. due to software restriction policy)	Success: **3038** (Device Guard), **8020** (AppLocker) Failure: **3077** (Device Guard) , **8022** (AppLocker)
Startup and shutdown of the RichOS, IE	Start-up: **4608**

Description	Context: Event ID (Detail) Note – *all* events are in the Security log.
System reboot, restart, and shutdown events (Success/Failure),	Shut-down: **1100**
Kernel module loading and unloading events (Success/Failure),	Success: **3038** (Other kernel modules), **Windows Boot Configuration Log** (Boot kernel module loading) Failure: **3004** (Other kernel modules), **Recovery Screen** (Boot kernel module loading)
Administrator or root-level access events (Success/Failure),	Success: **4624** Failure: **4625**

7.2 Audit events – WLAN client extended package

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

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

Requirement	Auditable Events	Additional Audit Record Contents	Log Name: Event ID (Detail)
FCS_TLSC_EXT.1/WLAN	Failure to establish an EAP-TLS session.	Reason for failure	System: **36888** Microsoft-Windows-CAPI2/Operational: **11, 30**
	Establishment/termination of an EAP-TLS session.	Non-TOE endpoint of connection.	System: **36880** (Establishment) Microsoft-Windows-SChannel-Events/Perf: **1793** (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: *detected integrity violation*].	[Selection: *The TSF binary file that caused the integrity violation*].	System: **20**

Requirement	Auditable Events	Additional Audit Record Contents	Log Name: Event ID (Detail)
FTA_WSE_EXT.1	All attempts to connect to access points.	Identity of access point being connected to as well as success and failures (including reason for failure).	Microsoft-Windows-WLAN-AutoConfig/Operational log event: **8001** (successful WLAN connection) **8002** (WLAN connection failure) **8003** (successful WLAN disconnection) **11004** (wireless network blocked) **11005** (wireless security succeeded) **11006** (wireless security failed) **12013** (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: **8001**, **8003**

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.

Event ID	Location in Log	Message	Fields
2		Package was successfully changed to the Installed state	**System**->**TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Security[UserID]**: <Subject identifier > **System->Level**: <Outcome as Success or Failure>
3		Windows update could not be installed because … "The data is invalid"	**Windows Logs->Setup**
11	**Microsoft-Windows-CAPI2/Operational**	Build Chain	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Level**: <Outcome as Success or Failure> **System->Security[UserID]**: <Subject identity> **UserData->Result**: <Reason for failure of validation>
20	**Windows Logs -> System**	The last boot's success was <LastBootGood event data>.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <type of event> **System-> Security[UserID]**: <subject identifier > **EventData->LastBootGood**: <Outcome as true or false indicating if the kernel-mode cryptographic self-tests and RNG initialization succeeded or failed>

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

Event ID	Location in Log	Message	Fields
3038	**Application and Services Logs->Microsoft->Windows->CodeIntegrity->Verbose**	Code Integrity started validaging image header of <kernel module pathname> file	**Application and Services Logs->Microsoft->Windows->CodeIntegrity->Operational**
3077	**Application and Services Logs->Microsoft->Windows->CodeIntegrity->Operational**	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.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Level**: <Outcome as Success or Failure> **System->Security[UserID]**: <Subject identifier>
4608	**Windows Logs->Security** Subcategory: Security State Change	Startup of audit functions	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **N/A**: <Subject identifier>
4624	**Windows Logs->Security** Subcategory: Logon	An account was successfully logged on.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->TargetUserSid**: <Subject identifier>

Event ID	Location in Log	Message	Fields
4625	**Windows Logs->Security** Subcategory: Logon	An account failed to log on.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->TargetUserSid**: <Subject identifier>
4656	**Windows Logs->Security** Subcategory: Handle Manipulation	A handle to an object was requested.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4670	**Windows Logs->Security** Subcategory: Policy Change	Permissions on an object were changed.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4673	**Windows Logs->Security** Subcategory: Sensitive Privilege Use	A privileged service was called.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>

Event ID	Location in Log	Message	Fields
4674	**Windows Logs->Security** Subcategory: Sensitive Privilege Use	An operation was attempted on a privileged object.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4720	**Windows Logs->Security** Subcategory: User Account Management	A user account was created.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4725	**Windows Logs->Security** Subcategory: User Account Management	A user account was disabled.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4726	**Windows Logs->Security** Subcategory: User Account Management	A user account was deleted.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>

Event ID	Location in Log	Message	Fields
4731	**Windows Logs->Security** Subcategory: User Account Management	A security-enabled local group was created.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4732	**Windows Logs->Security** Subcategory: User Account Management	A member was added to a security-enabled group.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4733	**Windows Logs->Security** Subcategory: User Account Management	A member was removed from a security-enabled group.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4734	**Windows Logs->Security** Subcategory: User Account Management	A security-enabled local group was deleted.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>

Event ID	Location in Log	Message	Fields
4735	**Windows Logs->Security** Subcategory: User Account Management	A security-enabled local group was changed.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4738	**Windows Logs->Security** Subcategory: User Account Management	A user account was changed	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4740	**Windows Logs->Security** Subcategory: Account Lockout	A user account was locked out.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4767	**Windows Logs->Security** Subcategory: Account Lockout	A user account was unlocked.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>

Event ID	Location in Log	Message	Fields
8001	**Microsoft-Windows-WLAN-AutoConfig/Operational**	WLAN AutoConfig service has successfully connected to a wireless network	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Level**: <Outcome as Success or Failure> **System->Security[UserID]**: <Subject identity> **EventData->PHYType, AuthenticationAlgorithm**: <Trusted channel protocol> **EventData->SSID**: <Non-TOE endpoint of connection>
8002	**Microsoft-Windows-WLAN-AutoConfig/Operational**	WLAN AutoConfig service failed to connect to a wireless network	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Level**: <Outcome as Success or Failure> **System->Security[UserID]**: <Subject identity> **EventData->PHYType, AuthenticationAlgorithm**: <Trusted channel protocol> **EventData->SSID**: <Non-TOE endpoint of connection>
8003	**Microsoft-Windows-WLAN-AutoConfig/Operational**	WLAN AutoConfig service has successfully disconnected from a wireless network	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Level**: <Outcome as Success or Failure> **System->Security[UserID]**: <Subject identity> **EventData->ConnectionId**: <Trusted channel protocol> **EventData->SSID**: <Non-TOE endpoint of connection>

Event ID	Location in Log	Message	Fields
8020	**Application and Services Logs->Microsoft->Windows->AppLocker->Packaged app-Execution**	<Packaged app name> was allowed to run.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Level**: <Outcome as Success or Failure> **System->Security[UserID]**: <Subject identifier>
8022	**Application and Services Logs->Microsoft->Windows->AppLocker->Packaged app-Execution**	<Packaged app name> was prevented from running.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Level**: <Outcome as Success or Failure> **System->Security[UserID]**: <Subject identifier>
11004	**Microsoft-Windows-WLAN-AutoConfig/Operational**	Wireless security stopped.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Level**: <Outcome as Success or Failure> **System->Security[UserID]**: <Subject identity> **EventData->SSID**: <Non-TOE endpoint of connection>
11005	**Microsoft-Windows-WLAN-AutoConfig/Operational**	Wireless security succeeded.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Level**: <Outcome as Success or Failure> **System->Security[UserID]**: <Subject identity> **EventData->SSID**: <Non-TOE endpoint of connection>

Event ID	Location in Log	Message	Fields
11006	**Microsoft-Windows-WLAN-AutoConfig/Operational**	Wireless security failed.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Level**: <Outcome as Success or Failure> **System->Security[UserID]**: <Subject identity> **EventData->SSID**: <Non-TOE endpoint of connection> **EventData->ReasonText**: <Failure condition> **EventData->ReasonCode**: <Failure condition error code>
12013	**Microsoft-Windows-WLAN-AutoConfig/Operational**	Wireless 802.1x authentication failed.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <Type of event> **System->Level**: <Outcome as Success or Failure> **System->Security[UserID]**: <Subject identity> **EventData->SSID**: <Non-TOE endpoint of connection>
36880	**Windows Logs -> System**	An TLS server handshake completed successfully. The negotiated cryptographic parameters are as follows:	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <type of event> **System->Security[UserID]**: <subject identifier > **UserData->EventXML->TargetName**: <Non-TOE endpoint>

Event ID	Location in Log	Message	Fields
36888	**Windows Logs -> System**	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.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <type of event> **System->Security[UserID]**: <subject identifier > **UserData->EventXML->TargetName**: <Non-TOE endpoint > **UserData->EventXML->AlertDesc:** < Reason for failure> **UserData->EventXML->ErrorState:** < Reason for failure > The following are the possible error codes: 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

8 Configuration Annex

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

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

8.1 Supported Configuration Actions

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

Configuration Action	NIST Control Reference	GP OS SFR	Specific Value for DoD or CNSSI 1253 (If Published)	Windows Management Method(s)	Admin Guide Reference
Configure Minimum Password Length to 12 Characters	IA-5 (1)(a)	FMT_MOF_EXT.1	12 characters	MDM Group Policy Command Line	6.7 Managing passwords and password policy
Require at Least 1 Special Character in Password	IA-5 (1)(a)	FMT_MOF_EXT.1	At least one	MDM Group Policy	6.7 Managing passwords and password policy
Require at Least 1 Numeric Character in Password	IA-5 (1)(a)	FMT_MOF_EXT.1	At least one	MDM Group Policy	6.7 Managing passwords and password policy
Require at Least 1 Uppercase Character in Password	IA-5 (1)(a)	FMT_MOF_EXT.1	At least one	MDM Group Policy	6.7 Managing passwords and password policy

Configuration Action	NIST Control Reference	GP OS SFR	Specific Value for DoD or CNSSI 1253 (If Published)	Windows Management Method(s)	Admin Guide Reference
Require at Least 1 Lowercase Character in Password	IA-5 (1)(a)	FMT_MOF_EXT.1	At least one	MDM Group Policy	6.7 Managing passwords and password policy
Enable Screen Lock	AC-11a	FMT_MOF_EXT.1		MDM Group Policy	6.10 Managing screen lock and session timeout
Set Screen Lock Timeout Period to 30 Minutes or Less	AC-11a	FMT_MOF_EXT.1	30 minutes	MDM Group Policy	6.10 Managing screen lock and session timeout
Disable Unauthenticated Login (such as Guest Accounts)	AC-11a	FIA_AFL.1		MDM Group Policy	6.7 Managing passwords and password policy
Set Maximum Number of Authentication Failures to 3 Within 15 Minutes	AC-7a	FMT_MOF_EXT.1	3 failures 15 minutes	MDM Group Policy Command Line	6.7 Managing passwords and password policy
Enable Host-Based Firewall	SC-7(12)	FMT_MOF_EXT.1		PowerShell	6.15 Managing the firewall
Configure Name/Address of Remote Management Server from Which to Receive Config Settings	CM-3(3)	FMT_MOF_EXT.1		MDM Group Policy	3.6 Modern device management 3.7 Approaches for configuring Windows policies
Configure the System to Offload Audit Records to a Log Server	AU-4(1)	FAU_GEN.1.1.c		*Not in scope for this GPOS evaluation per the Security Target.*	
Set Logon Warning Banner	AC-8a	FMT_MOF_EXT.1	See text below	MDM Group Policy Registry	6.11 Managing the logon banner

Configuration Action	NIST Control Reference	GP OS SFR	Specific Value for DoD or CNSSI 1253 (If Published)	Windows Management Method(s)	Admin Guide Reference
Audit All Logons (Success/Failure) and Logoffs (Successful)	AU-2a	FAU_GEN.1.1.c	Authentication events: (1) Logons (Success/Failure) (2) Logoffs (Success)	Group Policy Command Line	6.22 Managing audit policy
Audit File and Object Events (Unsuccessful)	AU-2a	FAU_GEN.1.1.c	File and object events: (1) Create (Success/Failure) (2) Access (Success/Failure) (3) Delete (Success/Failure) (4) Modify (Success/Failure) (5) Permission Modification (Success/Failure) (6) Ownership Modification (Success/Failure)	Group Policy Command Line	6.22 Managing audit policy

Configuration Action	NIST Control Reference	GP OS SFR	Specific Value for DoD or CNSSI 1253 (If Published)	Windows Management Method(s)	Admin Guide Reference
Audit User and Group Management Events (Success/Failure)	AU-2a	FAU_GEN.1.1.c	User and group management events: (1) User add, delete, modify, disable, enable (Success/Failure) (2) Group/Role add, delete, modify (Success/Failure)	Group Policy Command Line	6.22 Managing audit policy
Audit Privilege or Role Escalation Events (Success/Failure)	AU-2a	FAU_GEN.1.1.c	Privilege/Role escalation (Success/Failure)	Group Policy Command Line	6.22 Managing audit policy
Audit All Audit and Log Data Accesses (Success/Failure)	AU-2a	FAU_GEN.1.1.c	Audit and log data access (Success/Failure)	Group Policy Command Line	6.22 Managing audit policy
Audit Cryptographic Verification of Software (Success/Failure)	AU-2a	FAU_GEN.1.1.c		Group Policy Command Line	6.22 Managing audit policy
Audit Program Initiations (Success/Failure)	AU-2a	FAU_GEN.1.1.c	Application (e.g., Firefox, Internet Explorer, MS Office Suite, etc.) initialization (Success/Failure)	Group Policy Command Line	6.22 Managing audit policy
Audit System Reboot, Restart, and Shutdown Events (Success/Failure)	AU-2a	FAU_GEN.1.1.c	System reboot, restart and shutdown (Success/Failure)	Group Policy Command Line	6.22 Managing audit policy

Configuration Action	NIST Control Reference	GP OS SFR	Specific Value for DoD or CNSSI 1253 (If Published)	Windows Management Method(s)	Admin Guide Reference
Audit Kernel Module Loading and Unloading Events (Success/Failure)	AU-2a	FAU_GEN.1.1.c		Group Policy Command Line	6.22 Managing audit policy
Enable Automatic Software Update	SI-2	FMT_MOF_EXT.1		MDM Group Policy Command Line Windows GUI	6.13 Managing updates

8.1.1 Logon banner text

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

8.1.1.1 For DoD Systems:

```
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.
By using this IS (which includes any device attached to this IS), you consent to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to,
penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law
enforcement (LE), and counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring,
interception, and search, and may be disclosed or used for any USG-authorized purpose.
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for
your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or
monitoring of the content of privileged communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product
are private and confidential. See User Agreement for details.
```

8.1.1.2 For non-DoD NSS:

```
Organization-defined system use notification message or banner.
```