Microsoft

Operational and Administrative Guidance

Microsoft Windows Server, Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server 2019 version 1809 Hyper-V

Common Criteria Evaluation under the Protection Profile for Virtualization, including the Extended Package for Server Virtualization

Revision date: January 15, 2021

Copyright and disclaimer

1 Contents

2 Change history

Version	Date	Description
1.0	October 30, 2017	Windows 10, Server 2016, and Server 2012 R2 Virtualization Operational Guidance (Old Format)
2.0	December 15, 2019	Operational and Administrative Guidance: Microsoft Windows Server, Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server 2019 version 1809 Hyper-V

3 Introduction

This administrative guide provides information for Microsoft Windows Server, Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server 2019 version 1809 Hyper-V, as required by the Common Criteria Virtualization protection profile. All Windows Server and Windows 10 editions may be referred to collectively as "Windows" where appropriate. The goals of this administrative guide are to enable an IT professional to configure Windows and its operational environment to match the configuration under which the product was evaluated and to manage the Windows features in the scope of evaluation. The audience of this document is an IT Administrator familiar with current administrative practices for Windows 10. IT Administrators must follow the guidance in this document to ensure a device matches the evaluated configuration.

3.1 What's new

Since the last evaluation of Windows against the Common Criteria Virtualization protection profile, this administrative guide has been re-written in a new format.

3.2 How this guide is organized

The sections in this administrative guide group information together categorically:

- Section 3, Introduction, provides an overview of the guide, explains conventions in the document, and includes general guidance that the subsequent sections may refer back to.
- Section 4, Evaluated editions and platforms, identifies the specific editions of Windows 10 and Windows Server that were evaluated and the set of hardware platforms the evaluation was performed on.
- Section 5, Evaluated configuration, covers deployment of the product and the set of operational prerequisites and configuration choices that must be followed to match the evaluated Windows configuration.
- Section 6, Managing evaluated features, covers management of the Windows features in the scope of evaluation. This includes guidance on relevant feature configuration choices and approaches to implementing them, organized by feature area.
- Section 7, Audit events, provides detailed information on the audit events relevant to the evaluated configuration that are available in Windows logs. This information enables administrators to perform security monitoring and forensics.

3.3 Links to other resources

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

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

3.4 Security Target document

The Common Criteria evaluation requires a Security Target document that outlines the evaluation scope, which this guide may refer to. The correct matching Security Target for this administrative guide is the Microsoft Windows Server, Microsoft Windows 10 version 1909 (November 2019 Update), Microsoft Windows Server 2019 version 1809 Hyper-V 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

The evaluated configuration of Windows provides includes two roles that map to the Virtualization Protection Profile roles:

- **Administrator** – A local user account that is a member of either the Local Administrators or Hyper-V Administrators groups on the virtual host.
- **User** – A local user account that is neither a member of the Local Administrators group nor a member of the Hyper-V Administrators group. Standard Users have access to virtual machines, but not to most management functions.

See the Security Management section of the TOE Summary Specification in the Security Target document for a consolidated list that maps management functions to each role. In the introduction to each guidance section of this Administrative Guide, a table like the following identifies which role(s) the guidance applies to:

Role	Administrator 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 Standard User role.

The following articles describe local accounts in Windows and how to make a Standard User account a member of a local group, including the Local Administrators or Hyper-V Administrators groups:

- 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)

4 Evaluated editions and platforms

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

- Microsoft Windows Server Standard edition, version 1909
- Microsoft Windows Server Datacenter edition, version 1909
- Microsoft Windows Server 2019 Standard edition
- Microsoft Windows Server 2019 Datacenter edition
- Microsoft Windows 10 Enterprise edition, version 1909 (64-bit version)

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	Server Standard Server Datacenter Enterprise

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

- Dell PowerEdge R640
- Dell PowerEdge R7425
- Microsoft Surface Book 2

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. For Windows 10 Enterprise and Server editions in scope for this evaluation, 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 Security updates

For this evaluation, Windows 10 and Windows Server was evaluated with all critical updates available as of December 31, 2020 installed. See section 1 of the Security Target for related information. The current list of updates for this version of Windows is available at https://support.microsoft.com/en-us/help/4529964/windows-10-update-history.

The evaluated configuration also includes the Cumulative Update for Windows for November 2020, KB 4586819. This update may be downloaded directly from the Microsoft Update Catalog at https://www.catalog.update.microsoft.com/Search.aspx?q=4586819.

5.2.3 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.

5.2.4 FIPS 140 Approved cryptography mode

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

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

5.2.4.1 Configuring with Group Policy

Role	Administrator

Windows Editions	Server Standard Server Datacenter Enterprise

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).

5.2.4.2 Configuring with the Windows Registry

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

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

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

5.2.5 Additional cryptography configuration

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

- Support for TLS 1.0 must be explicitly disabled according to section 6.4.1, TLS versions in Windows.
- TLS ciphersuite selection must be configured according to section 6.4, Managing Transport Layer Security (TLS).
- SHA1 algorithms should be prioritized at the bottom of the algorithm negotiation list. See section 6.4, Managing Transport Layer Security (TLS), for implementation guidance.
- When using RSA schemes for key generation, RSA machine certificates must be configured with templates to use a minimum 2048-bit key length. See section 6.4.5, Configuring authentication schemes, for implementation guidance.
- IPsec VPN connections must be configured according to section 6.5.3, Configuring security association (SA) parameters for IPsec connections.

5.2.6 Device access configuration

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

- Complex passwords must be required. See section 6.6, Managing passwords and password policy, for implementation guidance.
- The password reveal button must be disabled. See section 6.6, Managing passwords and password policy, for implementation guidance.
- Session locking must be enabled. See section 6.7, Managing screen lock and session timeout, for implementation guidance.

5.2.7 Enabling virtualization features

To use any of the virtualization features covered in this evaluation, the device must have the Hyper-V role enabled. For specific instructions on enabling virtualization, see the section later in this document, Managing virtualization.

6 Managing evaluated features

6.1 Configuring Windows with Group Policy

Multiple sections of this guide refer to Windows policies, which may be configured using Group Policy solutions for domain-joined machines. For information on additional solutions to manage Hyper-V hosts remotely, see Managing Hyper-V Hosts Remotely. For information on how to join a

machine to a domain and add Active Directory users, see the following topics. Note that the directory server name and address to bind with must be supplied by your IT administrator.

- Join a Computer to a Domain: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/join-a-computer-to-a-domain
- Add users to a domain via New-ADUser: https://docs.microsoft.com/en-us/powershell/module/addsadministration/new-aduser?view=win10-ps

6.1.1 Setting policies with Group Policy Objects (GPO)

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

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).

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.

6.1.2 Setting policies with PowerShell and Group Policy Objects:

Role	Administrator

Windows Editions	Server Standard Server Datacenter Enterprise

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

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

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

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

6.2 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 when Windows is configured in FIPS 140 Approved cryptography mode as described in the Operational prerequisites section. 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 additional configuration. Keys are destroyed during Device Wipe.
- Windows generates asymmetric RSA keys using methods that meet FIPS-PUB 186-4 Appendix B.3, no additional configuration is necessary.
- Windows generates asymmetric ECC keys using methods that meet FIPS-PUB 186-4 Appendix B.4, no additional configuration is necessary.
- Windows performs RSA-based key establishment that meets NIST SP 800-56B, no additional configuration is necessary.
- Windows performs DSA-based key establishment that meets NIST SP 800-56B, no additional configuration is necessary.
- Windows performs elliptic curve-based key schemes that meet NIST SP 800-56A, no additional configuration is necessary.
- Windows generates random numbers according to NIST SP 800-90A, no additional configuration is necessary.
- Unprotected keys are not stored in non-volatile memory.

- Key lengths of keys used with certificates are configured in the certificate templates on the Certificate Authority used during enrollment and are not configured by the user or local administrator.
- There is no global configuration for hashing algorithms. The use of required hash sizes is supported. No additional configuration is necessary.
- Cryptographic Algorithm Validation Program (CAVP) testing was performed on the system cryptographic engine. Other cryptographic engines may have been separately evaluated but were not part of this Common Criteria evaluation.

6.3 Managing X.509 certificates

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

6.3.1 Client certificates and Certificate Authorities

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

Notes:

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

6.3.1.1 Configuring with the Certutil command line utility

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

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

6.3.1.2 Configuring with PowerShell

The PKIClient cmdlets enable a local administrator to complete a variety of tasks related to public key infrastructure (PKI), including importing a client certificate and creating a self-signed certificate for testing TLS mutual authentication. See the following topics for more information:

- PKIClient cmdlet reference: https://docs.microsoft.com/en-us/powershell/module/pkiclient/?view=win10-ps
- Import-Certificate: https://docs.microsoft.com/en-us/powershell/module/pkiclient/Import-Certificate?view=win10-ps
- New-SelfSignedCertificate: https://docs.microsoft.com/en-us/powershell/module/pkiclient/new-selfsignedcertificate?view=win10-ps

6.3.1.3 Configuring with the Windows UI

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

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

6.3.1.4 Configuring certificate request fields

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

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

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

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

6.3.2 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 (import) certificates to the store:

- Manage Trusted Root Certificates: https://technet.microsoft.com/en-us/library/hh945104.aspx

6.3.2.1 Configuring with group policy

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

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

6.3.2.2 Configuring with PowerShell

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

6.3.3 Certificate validation

Windows automatically compares the distinguished name (DN) in the certificate to the expected distinguished name and does not require additional configuration. The reference identifiers for TLS are the DNS name or IP address of the remote server (ID payload), which is compared against the DNS name as the presented identifier in either the Common Name or the Subject Alternative Name (SAN) of the certificate.

6.3.3.1 Configuring certificate validation for HTTPS in web browsers

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

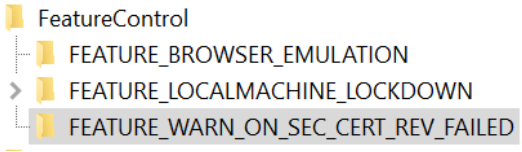
For Microsoft Edge: The administrator cannot configure certificate validation for HTTPS for Microsoft Edge. If the Web address does not match the certificate subject field, then the user is warned of a mismatch.

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

6.3.3.2 Configuring warnings in Internet Explorer when the certificate revocation service is unavailable

If Internet Explorer is unable to check a certificate's revocation status, for example, if no CRL or OCSP service is available, by default the browser will proceed to load the page without warning. Administrators may configure Internet Explorer to warn the user if the revocation check fails to complete by adding a key to the appropriate path in the Windows registry:

- Open the **Registry Editor** by typing **regedit** into the Windows search box or a command prompt
- Navigate to the registry path **Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl**
- Right-click on **FeatureControl** and choose **New > Key** to create a new registry key
- Name the registry key **FEATURE_WARN_ON_SEC_CERT_REV_FAILED**



- Right-click on the new key and choose **New > DWORD (32-bit) Value**
- Name the value **iexplore.exe**
- Double-click on the iexplore.exe value and set its **Value data** to **1**

Name	Type	Data
(Default)	REG_SZ	(value not set)
iexplore.exe	REG_DWORD	0x00000001 (1)

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

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

6.3.3.3 Certificate validation and code signing

The administrator cannot configure certificate validation for code signing purposes.

6.4 Managing Transport Layer Security (TLS)

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

6.4.1 Supported TLS versions and key establishment parameters in the evaluated configuration

Windows supports TLS protocol versions 1.0, 1.1, and 1.2. In its default configuration, all three versions of TLS are enabled in Windows, with TLS 1.2 set as the preferred protocol. A registry key provides administrators a solution to explicitly disable any version of TLS, e.g. 1.0. In the evaluated configuration, TLS 1.0 has been disabled. For more information on using the registry to control available TLS protocol versions, see the following topic:

- TLS Registry Settings: https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings

Windows supports a variety of key establishment schemes. Of these, the following are included in the evaluated configuration:

- Elliptic curves: secp256r1, secp384r1, and secp521r1. Note that secp521r1 is disabled by default, but still supported.
- Signature algorithms: SHA256, SHA384, and SHA512.

6.4.2 Available TLS ciphersuites

The ciphersuites listed in the Security Target correlate with those available in Windows 10 and Windows Server as noted in the table below. All ciphersuites listed are enabled by default, unless otherwise noted in the table. To enable ciphersuites that are not enabled by default, see the solutions for ciphersuite management listed in this guide, Configuring ciphersuites with PowerShell and Configuring ciphersuites with group policy.

Ciphersuites listed in the Security Target	Setting name (ciphersuite string) for the ciphersuite in Windows
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
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_SHA as defined in RFC 4492	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
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
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268	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

Ciphersuites listed in the Security Target	Setting name (ciphersuite string) for the ciphersuite in Windows
TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288	TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268	TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246	TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288	TLS_RSA_WITH_AES_256_GCM_SHA384

See the following article for additional information on TLS ciphersuites:

- TLS Cipher Suites in Windows 10 v1903, v1909, and v2004: https://docs.microsoft.com/en-us/windows/desktop/SecAuthN/tls-cipher-suites-in-windows-10-v1903.

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

6.4.3 Configuring ciphersuites with PowerShell

Administrators may manage TLS ciphersuites and elliptic curves using PowerShell cmdlets. In addition to enabling and disabling ciphersuites and elliptic curves, the cmdlets may also be used to specify a position in the priority list. The topics below provide more information on each cmdlet.

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

- Enable-TlsCipherSuite: https://docs.microsoft.com/en-us/powershell/module/tls/enable-tlsciphersuite?view=win10-ps
- Disable-TlsCipherSuite: https://docs.microsoft.com/en-us/powershell/module/tls/disable-tlsciphersuite?view=win10-ps
- Enable-TlsEccCurve: https://docs.microsoft.com/en-us/powershell/module/tls/enable-tlsecccurve?view=win10-ps
- Disable-TlsEccCurve: https://docs.microsoft.com/en-us/powershell/module/tls/disable-tlsecccurve?view=win10-ps

6.4.4 Configuring ciphersuites with group policy

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://docs.microsoft.com/en-us/windows/win32/secauthn/prioritizing-schannel-cipher-suites

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.

6.4.5 Configuring authentication schemes

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

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

- Cryptography (for configuring the algorithm that the issued certificate's key pair will support): https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770477(v=ws.11)
- 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_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289	Provider Category = Key Storage Provider

Ciphersuites (per Security Target)	Selections in the certificate template
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 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 TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288	Algorithm Name = RSA
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	Provider Category = Key Storage Provider Algorithm Name = ECDSA_P521

6.4.6 Managing signature algorithms and key length with the Windows registry

The signature algorithm and hash 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

To constrain the Diffie-Hellman key length, edit the following registry key:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman

With both registry keys, remove the algorithm(s) or key length(s) that should not be used. No additional algorithms other than the default set may be specified. For more information, see the following topic:

- TLS registry settings: https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings#keyexchangealgorithm---diffie-hellman-key-sizes

6.4.7 Configuring TLS mutual authentication

TLS mutual authentication is not enabled by default in IIS. To enable it, begin by installing the IIS Client Certificate Mapping Authentication role on the server. The following topic provides information on installing the IIS Client Certificate Mapping Authentication role via Server Manager.

- IIS Client Certificate Mapping Authentication: https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/authentication/iisclientcertificatemappingauthentication/

Also using Server Manager, two options for the website must be set to enable TLS mutual authentication:

- Require SSL
- Require Client Certificate

Next, configure many-to-one client certificate mapping on the server. The following topic explains how to do this using IIS Configuration Editor:

- Configure Many-to-One Client Mappings: https://docs.microsoft.com/en-us/troubleshoot/iis/configure-many-to-one-client-mappings

Finally, appropriate client certificates must be distributed to clients. The recommendation is to configure user certificate auto-enrollment on the domain server where Active Directory Domain Services (AD DS) is installed, then join the client computer to the same domain. After joining the

domain and connecting to the server, e.g., with a browser, the user will be prompted to confirm and select the certificate provided by AD DS. Note that:

- Key strength for key establishment follows the certificate strength provided by the server.
- No configuration is needed besides enabling auto-enrollment with the certificate templates desired.
- The configuration is the same for different types of certificates.

The following topic provides information on configuring user certificate auto-enrollment:

- Configure certificate auto-enrollment: https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/configure-server-certificate-autoenrollment

For more information on managing client certificates and information on configuring certificate templates, see the section, Client certificates and Certificate Authorities.

6.4.8 Choosing TLS in a web browser

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

6.4.9 Securing LDAP with TLS (LDAP-S)

Administrators may secure Lightweight Directory Access Protocol (LDAP) connections in an Active Directory environment with TLS. Enabling LDAP signing (LDAP-S) is the preferred solution for this. The following topic provides an overview of the technology and solutions to implement it that leverage Group Policy, local computer policy, and the Windows registry:

- How to enable LDAP signing in Windows Server: https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/enable-ldap-signing-in-windows-server

6.5 Managing IPsec and VPN connections

Role	All

Windows Editions	Server Standard Server Datacenter Enterprise

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

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

Note:

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

6.5.1 Configuring IPsec firewall rules using Windows Defender Firewall with Advanced Security

The Windows Filtering Platform (WFP) is the IPsec Security Policy Database (SPD) for Windows. WFP starts automatically with Windows and must always be running to support IPsec scenarios. WFP features, including IPsec configuration, are exposed through the Windows Defender Firewall with Advanced Security features, which can be configured through the Windows Firewall with Advanced Security user interface, by Group Policy, or with PowerShell. The following articles introduce how WFP operates and provide an overview of the IPsec configuration it enables:

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

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

- **Protect**: create a custom Outbound Rule, using the following parameters as a model:
  - Create a new outbound rule.
  - Choose protocol type: TCP.

- Set the appropriate remote port, e.g. 8080.
- Set the appropriate remote IP addresses the rule applies to, e.g. 192.168.5.102 and 192.168.4.0/24.
- Select Allow the connection if it is secure.
- Select Customize.
- Select Allow the connection if it is authenticated and integrity-protected and click OK.
- Select all domains.
- Give the rule a name, e.g. ProtectRule2 and confirm the operation.

- **Bypass**: create a Connection Security Rule, similar to an Authentication Exemption List rule except with the following parameters:
  - Type: Server to Server.
  - Choose to require authentication for inbound connections.
  - Choose to request authentication for outbound connections.

- **Discard**: create a custom Inbound Rule with the action to block the connection.

Rules may be created using the Windows user interface, Group Policy, or PowerShell; see the subsections below for more information. The different solutions for creating rules listed in the following subsections provide control over the order in which they are executed.

The following articles provide additional information on configuring common rules:

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

6.5.1.1 Configuring with the user interface

Role	Local Administrator

Windows Editions	Server Standard Enterprise

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

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

6.5.1.2 Configuring with Group Policy

Role	IT Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

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

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

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

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

6.5.1.3 Configuring with PowerShell

Role	Local Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

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

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

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

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

6.5.2 Configuring and using VPN connections and the VPN client

Windows Editions	Server Standard Server Datacenter Enterprise

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

Notes on IPsec VPN configuration limitations:

- To prevent standard users from modifying or deleting IPsec VPN connections, administrators may use the -AllUserConnection parameter when creating or configuring the connection profile, as described in section 6.5.2.1, Configuring VPN using PowerShell.
- Windows supports Network Address Translation (NAT) traversal automatically as part of the IKEv1 and IKEv2 protocols. No configuration is needed or possible.
- Security association lifetime settings for IKEv2 may only be configured on the VPN gateway. No client configuration is needed or possible in the VPN client.
- For IKEv1 connections, Windows supports only main mode. It is not possible to configure IKEv1 to use aggressive mode.
- For IKEv1 connections, XAUTH is not supported.
- When using a pre-shared key, the secret value input into the client must match the secret value configured on the VPN server. The key must be at least 22 characters in length, but less than 256 characters. The key may be composed of any combination of upper and lower case letters, numbers, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")".

6.5.2.1 Configuring VPN using PowerShell

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

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

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

The Add-VpnConnection and Set-VpnConnection cmdlets may be used to add new IPsec VPN connections and to specify their connection type (e.g., IKEv1 / L2TP, IKEv1 / L2TP with a pre-shared key, or IKEv2), the tunnel type (PPTP or L2TP in the evaluated configuration), the authentication method (e.g., PAP, CHAP, MSCHAPv2, EAP, or machine certificates), and many more parameters. Note: when using IKEv1 with a pre-shared key, the key is generated by the user or administrator. The -AllUserConnection parameter may be used to store the IPsec VPN connection in the global phone book, making it available to all users and preventing standard users from deleting or modifying it. The following articles provide more information on Add-VpnConnection and Set-VpnConnection:

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

The Set-VpnConnectionIPsecConfiguration cmdlet may be used to specify additional IPsec parameters, including the ESP encryption algorithm (AES-GCM-128, AES-GCM-256, AES-CBC-128, and AES-CBC-256 in the evaluated configuration), Diffie-Hellman (DH) group (DH Groups 14, 19, 20, or 24 in the evaluated configuration). The following article provides more information on Set-VpnConnectionIPsecConfiguration:

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

6.5.2.2 Configuring a new VPN connection with the Windows UI

Role	User
Windows Editions	Server Standard Server Datacenter Enterprise

The following steps outline how to create and configure a new connection in the Windows RAS IPsec VPN client, including choosing options for IKEv1, IKEv1 with a pre-shared key, and IKEv2. The UI in the RAS IPsec VPN client supports the limited configuration options listed below; to configure more aspects of a VPN connection, use the PowerShell cmdlet solutions.

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

- For IKEv2, from **VPN type** choose the **IKEv2** option and choose **Certificate** as the type of sign-in info (see the additional note below if using machine certificates)
- Choose the authentication method from **Type of sign-in info**
- Configure the user credentials as appropriate
- **Save** the connection
- **Note if using machine certificates:** To configure the VPN connection to use machine certificates, you must adjust the properties via the Adapter Properties feature.
  - Open **Network Connections** from the Control Panel (or, choose **Change adapter options** from the VPN panel in Settings).
  - Right-click on the VPN connection and select **Properties**.
  - Select the **Security** tab.
  - Select the **Use machine certificates** option.

6.5.2.3 Connecting to a VPN gateway with the Windows UI

Role	User
Windows Editions	Server Standard Server Datacenter Enterprise

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

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

6.5.2.4 VPN client security association lifetime

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

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

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

6.5.3 Configuring security association (SA) parameters for IPsec VPN connections

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

Notes on supported algorithms in the evaluated configuration:

- The following encryption algorithms are supported in the evaluated configuration: AES-GCM-128, AES-GCM-256, AES-CBC-128, and AES-CBC-256. Of those, only AES-CBC-128 and AES-CBC-256 can be used for IKEv1 and IKEv2 connections.
- For IKEv1 connections, the strength of the AES algorithm used for Phase 1 must be equal to or greater than the strength of the algorithm used for Phase 2. For IKEv2 connections, the strength of the AES algorithm used for the IKE_SA must be equal to or greater than the strength of the algorithm used for IKE_SA2. These attributes may be configured using Set-VpnConnectionIPsecConfiguration, as described in section 6.5.2.1, Configuring VPN using PowerShell, or configured and deployed using ProfileXML, as described in section 6.5.3.1, Configuring IPsec VPN connections using Profile XML.
- The following authentication algorithms are supported in the evaluated configuration: HMAC-SHA1, HMAC-SHA-256, and HMAC-SHA-384; Diffie-Hellman Groups 14, 19, 20, and 24.
- The following signature algorithms are supported in the evaluated configuration: RSA, ECDSA P256, and ECDSA P384

6.5.3.1 Configuring IPsec VPN connections using Profile XML

A ProfileXML file may be used to configure multiple attributes of an IPsec VPN connection, including those noted above in section 6.5.3 as part of the evaluated configuration. An administrator may lock these settings by setting the Lockdown element to Yes within the ProfileXML. The following topic provides an overview of ProfileXML and its deployment:

- Configure Windows 10 Client Always On VPN Connections – Profile XML Overview: https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/vpn-deploy-client-vpn-connections#profilexml-overview

6.5.3.2 Configuring IPsec in transport or tunnel mode

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

Windows supports transport mode security associations (SAs) via the IKEv2 protocol. When configuring an IPsec connection using one of the solutions in the section, Configuring and using VPN connections and the VPN client, choose IKEv2 for transport mode. The following topic provides additional detail on securing IPsec connections using IKEv2:

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

Windows supports tunnel mode SAs via the Layer 2 Tunneling Protocol (L2TP). When configuring an IPsec connection using one of the solutions in the section, Configuring and using VPN connections and the VPN client, choose L2TP for tunnel mode.

For additional information about IPsec transport and tunnel mode scenarios in Windows, see the following topics:

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

6.5.3.3 Configuring IKEv1 security association lifetime using PowerShell

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

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

PowerShell cmdlets:

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

PowerShell configuration of quick mode:

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

6.5.3.4 Configuring authentication signature algorithms

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

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

- RSA
- ECDSA P256
- ECDSA P384

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

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

The SubjectName and SubjectNameType options combined with the ValidationCriteria option for the New-NetIpsecAuthProposal cmdlet are used to configure how the name of the remote certificate will be verified. Use the DomainName value for the SubjectNameType parameter to configure either a domain name (DN) or fully qualified domain name (FQDN). Use the CommonName value for the SubjectNameType to configure an IP address. In addition, the RemoteAddress and SubjectName options for the New-NetIpsecAuthProposal cmdlet must be set to the IP address in the certificate.

6.5.3.5 Configuring certificate validation and revocation checks

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

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

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

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

6.5.3.6 Using pre-shared keys

Role	Local Administrator, IT Administrator

Windows Editions	Server Standard Server Datacenter Enterprise

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

6.6 Managing virtualization

The following sections describe management functions related to virtualization. In some cases, the solutions to enable or manage virtualization features are different between Windows 10 and Windows Server. See the section title and the table in each section's introduction for details on what solutions apply to which Windows editions.

6.6.1 Enabling and updating virtualization features

6.6.1.1 Enabling virtualization on Windows 10 using Windows Features, PowerShell, or the command line

Role	Administrator
Windows Editions	Enterprise

The virtualization features are not enabled by default on Windows 10 Enterprise. First, check that the Windows 10 system meets the minimum requirements for Hyper-V, as documented in the following topic:

- Windows 10 Hyper-V System Requirements: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements

A local administrator may use the Windows Features settings, PowerShell cmdlets, or a command line tool to enable the Hyper-V role and the virtualization features that accompany it. The following topic provides information on these solutions:

- Install Hyper-V on Windows 10: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v

On some devices, support for virtualization must also be enabled via the device bios. Refer to the specific device specifications and documentation for related information.

6.6.1.2 Enabling virtualization on Windows Server using Server Manager or PowerShell

Role	Administrator
Windows Editions	Server Standard Server Datacenter

First, check that the Windows Server system meets the minimum requirements for Hyper-V, as documented in the following topic:

- System requirements for Hyper-V on Windows Server: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/system-requirements-for-hyper-v-on-windows

To create and run virtual machines on Windows Server, the Hyper-V role must be installed. This may be achieved using Server Manager or with PowerShell cmdlets. The following topic provides information on both solutions:

- Install the Hyper-V role on Windows Server: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server

6.6.1.3 Updating the virtualization system using Hyper-V Manager or PowerShell

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

Updating the Hyper-V virtualization system is a separate but related action from managing Windows updates. For information on Windows updates, see the section, Managing updates. When a Hyper-V host is upgraded to the latest version of Windows or Windows Server (via Windows Update or another mechanism), an administrator may use either Hyper-V Manager or PowerShell to upgrade the Hyper-V configuration version for the hosted VMs. The following topic provides information on both upgrade solutions:

- Upgrade virtual machine version in Hyper-V on Windows 10 or Windows Server: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/upgrade-virtual-machine-version-in-hyper-v-on-windows-or-windows-server#step-2-upgrade-the-virtual-machine-configuration-version

6.6.2 Managing Hyper-V Hosts Remotely

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

Hyper-V supports three methods of remote administration:

- Hyper-V Manager
- PowerShell
- Remote Desktop (RDP)

Remote administrators must logon to the remote administration interfaces using administrator credentials in order to perform the management functions listed in this administrative guide. The following topics provide information on the remote management solutions for Hyper-V hosts:

- Remotely manage Hyper-V hosts with Hyper-V Manager: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/manage/remotely-manage-hyper-v-hosts
- Working with Hyper-V and Windows PowerShell: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/try-hyper-v-powershell

- Remote Desktop Services overview, planning, implementation, and management: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds

6.6.3 Creating and configuring virtual machines

The following sections provide details on creating and configuring virtual machines. In most situations, it is advisable to create a virtual switch to support networking of VMs before creating the VMs themselves. See the section Managing virtual networking for instructions on virtual switches.

6.6.3.1 Creating and configuring VMs on Windows 10 using Hyper-V Quick Create

Role	Administrator User
Windows Editions	Enterprise

Hyper-V Quick Create is a desktop app that may be used independently from Hyper-V Manager on Windows 10 Enterprise edition. Hyper-V Quick Create enables quick VM creation with limited options to name the VM and choose a virtual switch for networking. If you require options beyond these, use PowerShell for VM creation. The following topic provides instructions for Hyper-V Quick Create:

- Create a Virtual Machine with Hyper-V: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/quick-create-virtual-machine

6.6.3.2 Creating and configuring VMs using Hyper-V Manager or PowerShell

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

Hyper-V Manager and PowerShell provide a rich set of VM management functions, including creating and configuring new VMs. Both Hyper-V manager and PowerShell are available on Windows Enterprise and Server editions. The following topic provides instructions for both solutions:

- Create a virtual machine in Hyper-V: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/create-a-virtual-machine-in-hyper-v

The following topics provide additional details and context for using PowerShell to create and configure VMs:

- Hyper-V and PowerShell: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/try-hyper-v-powershell
- New-VM PowerShell cmdlet: https://docs.microsoft.com/en-us/powershell/module/hyper-v/new-vm?view=win10-ps

6.6.4 Deleting virtual machines

6.6.4.1 Delete VMs using Hyper-V Manager

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

Hyper-V Manager provides many management functions for VMs hosted on a server, including the ability to delete VMs. Note that deleting a VM does not remove any virtual hard drives associated with the VM. To delete an existing VM using Hyper-V Manager, follow these steps:

- Open **Hyper-V Manager**
- Select the **Hyper-V Host** that hosts the VM from the list of hosts in the left pane.
- Select the VM to delete from the list of **Virtual Machines** in the middle pane. If the VM is currently running, shut it down.
- To delete the VM and its associated files, choose **Delete…** from the **Actions** pane on the right.
- Confirm the operation.

6.6.4.2 Delete VMs using PowerShell

Role	Administrator

Windows Editions	Server Standard Server Datacenter Enterprise

PowerShell may be used to delete an existing VM from a Hyper-V host using the Remove-VM cmdlet. Note that Remove-VM does not remove any virtual hard drives associated with the VM. To remove a virtual hard drive from a VM before deleting the VM, use the Remove-VMHardDiskDrive cmdlet. The following topics provide detailed information on the PowerShell cmdlets:

- Remove-VM: https://docs.microsoft.com/en-us/powershell/module/hyper-v/remove-vm?view=win10-ps
- Remove-VMHardDiskDrive: https://docs.microsoft.com/en-us/powershell/module/hyper-v/remove-vmharddiskdrive?view=win10-ps

6.6.5 Managing virtual networking using Hyper-V Manager or PowerShell

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

Virtual machine networking is enabled by creating and managing a Hyper-V Virtual Switch, which can be accomplished either using the Virtual Switch Manager within Hyper-V Manager, or via PowerShell cmdlets. The same methods are used regardless of whether the scenario is VM to VM, VM to Internet, or VM to physical network. Multiple networks or subnets may be created using the same means to separate operational and administrative networks. The following topics provide an overview of the Hyper-V Virtual Switch and how to manage it:

- Create a virtual switch for Hyper-V virtual machines (Windows Server editions, Windows 10 Enterprise): https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/create-a-virtual-switch-for-hyper-v-virtual-machines
- Create a virtual network (Windows 10 Enterprise): https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/connect-to-network

The following topics provide additional details on the features available in Hyper-V Virtual Switch and options for managing them:

- Hyper-V Virtual Switch: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v-virtual-switch/hyper-v-virtual-switch

- Manage Hyper-V Virtual Switch: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v-virtual-switch/manage-hyper-v-virtual-switch

The following topic provides additional details on the PowerShell cmdlet used to create a Hyper-V Virtual Switch:

- New-VMSwitch: https://docs.microsoft.com/en-us/powershell/module/hyper-v/new-vmswitch?view=win10-ps

6.6.6 Configuring initial defaults for creating new VMs

The initial default settings used by Hyper-V Manager, PowerShell, or Hyper-V Quick Create to create new VMs may not be customized. Instead, Windows offers solutions to create a VM template that may be used to quickly create VMs with a specific configuration.

6.6.6.1 Adding custom VMs to the Hyper-V Quick Create virtual machine gallery

Role	Administrator
Windows Editions	Enterprise

The Hyper-V Quick Create app includes a virtual machine gallery that provides a choice of virtual machine sources defined in the Windows registry. This gallery may be populated with custom images, enabling quick creation of VMs based on the images. The following topic provides more information:

- Create a custom virtual machine gallery: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/custom-gallery

6.6.6.2 Export and import virtual machines using Hyper-V Manager or PowerShell

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

Exporting and importing a VM is the recommended solution for moving or copying a VM. Exported VMs may be used as templates to create new VMs that match the exported VM configuration. Both Hyper-V Manager and PowerShell provide solutions for exporting and importing VMs. The following topics provide an overview of import and export, as well as details on the PowerShell cmdlets involved:

- Export and import virtual machines: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/deploy/export-and-import-virtual-machines
- Export-VM cmdlet: https://docs.microsoft.com/en-us/powershell/module/hyper-v/export-vm?view=win10-ps
- Import-VM cmdlet: https://docs.microsoft.com/en-us/powershell/module/hyper-v/import-vm?view=win10-ps

Depending on the scenario, an administrator may choose to generalize a VM image before exporting it for use as a template, removing unique information from the Windows installation so that the image can better be used as a template for other VMs. The Sysprep command-line tool and its VM mode of operation may be used to generalize VM images. The following topics provide more information on Sysprep and its use for VM image generalization:

- Sysprep (Generalize) a Windows Installation: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/sysprep--generalize--a-windows-installation
- Sysprep Command-Line Options: https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/sysprep-command-line-options
- Sysprep /mode:vm switch: https://blogs.technet.microsoft.com/tip_of_the_day/2013/09/26/tip-of-the-day-syspreps-new-modevm-switch/

6.6.7 Sharing data between VMs and sharing devices with VMs

Windows Editions	Server Standard Server Datacenter Enterprise

6.6.7.1 Networking VMs to share data

Role	Administrator

Data may be shared between VMs by using virtual network adapters for VM to VM communications. See the resources in the previous section,

Managing virtual networking using Hyper-V Manager or PowerShell, for more information on creating and configuring virtual networks. All three types of virtual network (private, internal, and external) provide the connected VMs network access to each other. Once VMs are connected to the same network, the standard Windows sharing and access controls may be used to grant permissions to resources.

6.6.7.2 Sharing devices with VMs and enabling copy-and-paste data sharing

Role	Administrator User

Enhanced Session Mode enables local resources, including devices, to be shared with VMs, and enables copy-and-paste data sharing between machines. To enable these scenarios, Enhanced Session Mode must be enabled on the VM host and the user must select specific options when connecting to the VM using the Remote Desktop Client (RDP).

Either Hyper-V Manager or PowerShell may be used to enable Enhanced Session Mode. For more information on enabling Enhanced Session Mode, see the following topics:

- Use local resources on Hyper-V virtual machine with VMConnect: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/learn-more/use-local-resources-on-hyper-v-virtual-machine-with-vmconnect
- Set-VMHost cmdlet (see -EnableEnhancedSessionMode parameter): https://docs.microsoft.com/en-us/powershell/module/hyper-v/set-vmhost?view=win10-ps

Once Enhanced Session Mode is enabled for VMs on a host, data and device sharing for a session is enabled by connecting to a VM using RDP with the Enhanced Session Mode options enabled. In this way, resources on the VM host may also be shared with the VM. For more information on connecting to a VM via RDP with these options, see the following topic:

- Share devices with your virtual machine: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/user-guide/enhanced-session-mode

6.6.8 Managing physical platform resources using Hyper-V Manager or PowerShell

Role	Administrator

Windows Editions	Server Standard Server Datacenter Enterprise

By default, a guest VM is allowed access to the virtualized processor, virtualized physical memory, and virtualized TPM of the host; access to all other physical platform resources on the host is denied. Device access, including for removable media devices, may be added to VMs using Hyper-V Manager or PowerShell. For example, a VM may be enabled to read a DVD .iso image by adding a virtual DVD drive to the VM. Note that a hard disk drive may also be removable media, e.g., an inserted USB drive.

Within Hyper-V Manager, devices may be added via VM Settings:

- Open **Hyper-V Manager**
- Select the **Hyper-V Host** that hosts the VM from the list of hosts in the left pane
- Select the desired VM from the list of **Virtual Machines** in the middle pane
- Select **Settings…** from the **Actions** pane on the right
- Choose **Add Hardware** and select the appropriate options. For the DVD drive example mentioned above, first add a SCSI controller and then add a DVD drive to it.
- Confirm the operation

PowerShell exposes cmdlets specific to different types of virtual devices. The topics below provide a reference of all Hyper-V PowerShell cmdlets and specific information for common virtual device scenarios:

- Hyper-V cmdlet reference: https://docs.microsoft.com/en-us/powershell/module/hyper-v/?view=win10-ps
- Add-VMScsiController: https://docs.microsoft.com/en-us/powershell/module/hyper-v/Add-VMScsiController?view=win10-ps
- Add-VMDvdDrive: https://docs.microsoft.com/en-us/powershell/module/hyper-v/Add-VMDvdDrive?view=win10-ps
- Add-VMHardDiskDrive: https://docs.microsoft.com/en-us/powershell/module/hyper-v/Add-VMHardDiskDrive?view=win10-ps

6.6.9 Managing VMs from a host

Role	Administrator User

Windows Editions	Server Standard Server Datacenter Enterprise

6.6.9.1 Manage VMs with Hyper-V Manager

Hyper-V Manager provides a wide variety of functions to control and manage VMs. Within Hyper-V Manager, these are exposed in the Action pane, after a VM has been selected. These actions include common functions such as starting, stopping, suspending, and checkpointing a VM:

- Open **Hyper-V Manager**
- Select the **Hyper-V Host** that hosts the VM from the list of hosts in the left pane
- Select the desired VM from the list of **Virtual Machines** in the middle pane
- Choose the appropriate function from the **Actions** pane on the right
- Confirm the operation

6.6.9.2 Manage VMs with PowerShell

PowerShell exposes VM control and management functions via cmdlets specific to each task. The topics below provide a reference of all Hyper-V PowerShell cmdlets and specific information for common functions such as starting, stopping, suspending, and checkpointing a VM:

- Hyper-V cmdlet reference: https://docs.microsoft.com/en-us/powershell/module/hyper-v/?view=win10-ps
- Start-VM cmdlet: https://docs.microsoft.com/en-us/powershell/module/hyper-v/Start-VM?view=win10-ps
- Stop-VM cmdlet: https://docs.microsoft.com/en-us/powershell/module/hyper-v/Stop-VM?view=win10-ps
- Suspend-VM cmdlet: https://docs.microsoft.com/en-us/powershell/module/hyper-v/Suspend-VM?view=win10-ps
- Resume-VM cmdlet: https://docs.microsoft.com/en-us/powershell/module/hyper-v/resume-vm?view=win10-ps
- Checkpoint-VM cmdlet: https://docs.microsoft.com/en-us/powershell/module/hyper-v/Checkpoint-VM?view=win10-ps

6.6.9.3 Manage VMs with PowerShell Direct

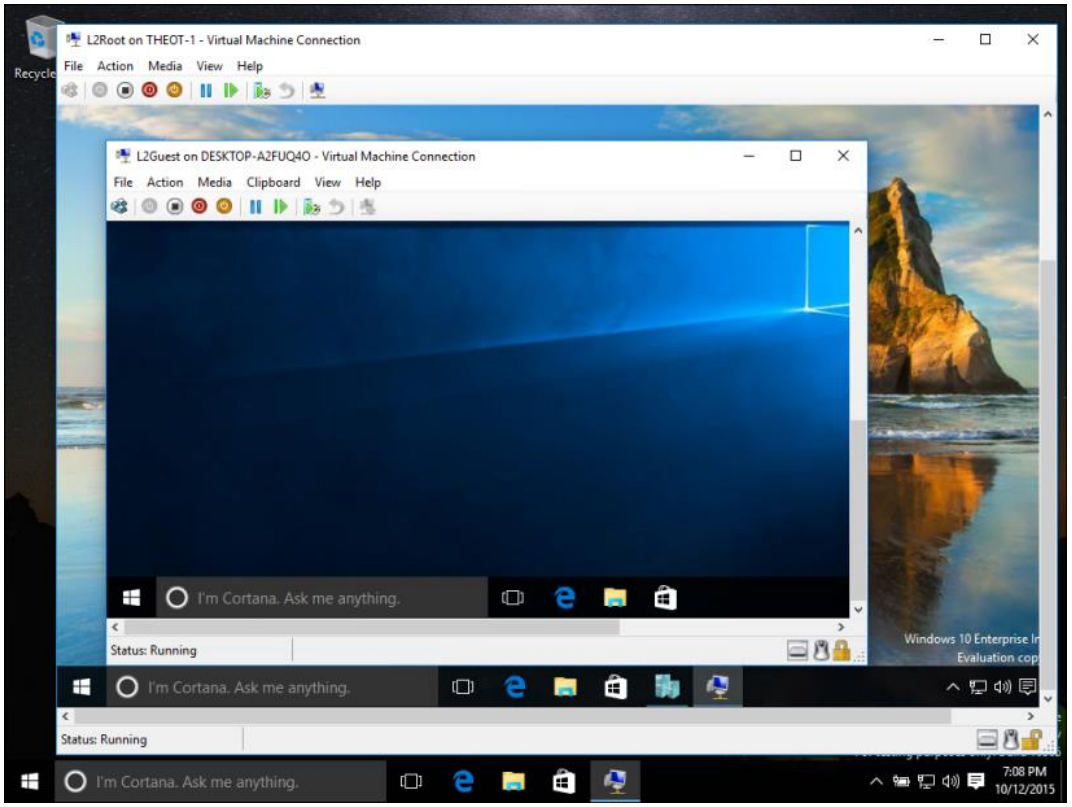
PowerShell direct provides a solution to remotely manage VMs from a Hyper-V host, including Windows Server Datacenter without the Desktop Experience installed. With PowerShell direct, an administrator may create a remote session with a VM and run PowerShell commands or scripts on the VM. For more information, see the following topic:

- Manage Windows virtual machines with PowerShell Direct: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/manage/manage-windows-virtual-machines-with-powershell-direct

6.6.10 Indicating input focus for VM clients

Role	Administrator User
Windows Editions	Server Standard Server Datacenter Enterprise

The Hyper-V client user interface indicates which virtual machine is connected to the physical keyboard and mouse. The screen shot below shows two VM clients running, both of which have access to keyboard and mouse, as indicated by the keyboard and mouse icons in the lower-right corner of each VM client window. In this scenario, the Hyper-V client window in focus (i.e., the active window) is the virtual machine with input focus.



6.6.11 Managing hardware-based isolation mechanisms

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

Hardware-based isolation mechanisms are enabled by default for all systems that meet the Hyper-V system requirements. No configuration is necessary. The following topics provide detailed information on the Hyper-V system requirements:

- System requirements for Hyper-V on Windows Server: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/system-requirements-for-hyper-v-on-windows
- System requirements for Hyper-V on Windows 10 Enterprise: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements

6.6.12 Hypercall controls and the Hypervisor interface

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

The Hypervisor provides a documented interface for virtual machines to invoke. An administrator enables VMs to use the hypercall interface by installing an enlightened operating system as the guest operating system. An administrator may block the hypercall interface by installing an unenlightened operating system as the guest operating system. No additional configuration is possible. The following specifications provide the public documentation of the Hypervisor hypercall interface – see the Hypercall Interface section of each:

- Hypervisor Top-Level Functional Specification for Windows Server 2019 (v6.0b), available at https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/tlfs
- Hypervisor Top-Level Functional Specification for Windows Server 2016 (v5.0c), available at https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/tlfs

6.7 Managing authentication methods

The following sections provide multiple options for managing user authentication in Windows.

Notes

- Services provided before logon are automatically limited, no configuration is necessary.
- For general best practices on setting password complexity, see the topic, Password must meet complexity requirements: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

6.7.1 Configuring authentication, password, and PIN policies with group policy

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

Authentication policies, including password and Windows Hello PIN policies, may be configured using group policy. The following topics provide a sample of Account Policy functions that address common needs of IT administrators. The linked topics provide detailed information on the policy function and how to implement it.

- Configuring Windows to require a smart card or Windows Hello factor for interactive logon: Use the setting **Interactive logon: Require smart card** 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-require-smart-card.
- 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 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.

The Password Policy set, part of the larger Account Policies, provide a variety of group policy management functions for password policy. The following sample of Password Policy functions addresses the common needs of IT administrators. The linked topics provide detailed information on the policy function and how to implement it.

- Overview of group policies available in the Password Policy set: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/password-policy

- Specifying password length: Use the setting **Minimum password length** under **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy**. Note that the largest minimum length supported with this GPO is 14 characters. To configure a minimum length above 14, use the net.exe solution. 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 password expiration: Use the setting **Maximum password age** under **Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy.** For more information, see: https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/maximum-password-age.
    - Disabling the password reveal button: Use the setting **DisablePasswordreveal** under **Computer Configuration\Administrative Templates\Windows Components\Credential User Interface.**

Windows Hello PIN, i.e., a combination of username and PIN, may be configured via group policy. The relevant policy is:

- **Turn on Windows Hello PIN sign-in** under **Computer Configuration\Administrative Templates\System\Logon**

6.7.2 Configuring account and password policies with net.exe accounts utility

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

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.

6.7.3 Configuring a Windows Hello PIN with the Windows UI

Role	User
Windows Editions	Enterprise

To enable a Windows Hello PIN in place of passwords, follow the steps below. Note that a Windows Hello PIN may only be used for local interactive logon.

- 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

6.7.4 Configuring smart card logon

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

- How Smart Card Sign-in Works in Windows: https://docs.microsoft.com/en-us/windows/security/identity-protection/smart-cards/smart-card-how-smart-card-sign-in-works-in-windows
- Get started with Virtual Smart Cards: Walkthrough Guide: https://docs.microsoft.com/en-us/windows/security/identity-protection/virtual-smart-cards/virtual-smart-card-get-started

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

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

6.7.5 Logging on as an administrator

The Windows welcome screen provides administrators access to interactive logon for all authentication methods.

- From the welcome screen, press **any key** to log on. Windows defaults to the last user account and authentication method used.
- To choose a different authentication method, choose **Sign-in options** from the welcome screen and select from the authentication methods enabled on the device.
- To choose a different user account, select an account from the list of users in the corner of the welcome screen. On a domain-joined machine, choose **Other user** to enter the credentials of a different domain user.

The following topic provides additional detail on local Windows accounts, including the Administrator account:

- Local accounts: https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/local-accounts

6.8 Managing screen lock, session timeout, and TPM lockout

Role	Administrator

Windows Editions	Server Standard Server Datacenter Enterprise

6.8.1 Configuring screen lock and session timeout with group policy

Screen lock and session timeout for interactive logon (local or remote) 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.

6.8.2 Configuring screen lock and session timeout with the Windows registry

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

6.8.3 Configuring TPM lockout

TPM lockout, e.g. for smart card authentication scenarios, may be managed by the TPM MMC, Group Policy, or PowerShell. See the following topic for more information on the solutions available for managing TPM lockout:

- Manage TPM lockout: https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/manage-tpm-lockout

6.9 Managing the logon banner

Role	Administrator

Windows Editions	Server Standard Server Datacenter Enterprise

6.9.1 Configuring with group policy

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

6.9.2 Configuring with the Windows registry

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

6.10 Managing Windows Time Service Tools

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

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

6.11 Managing updates

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

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

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

6.11.1 Configuring using group policy

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

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

6.11.2 Configuring using the Server Configuration tool

Role	Administrator

Windows Editions	Server Standard Server Datacenter

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

6.11.3 Checking for available and installed updates using the Windows UI

Role	Administrator User
Windows Editions	Server Standard Server Datacenter Enterprise

To manually check for available Windows updates, follow these steps:

- Open **Settings**
- Navigate to **Update & Security**
- Choose **Windows Update** from the categories in the left navigation
- Click the **Check for updates** button

To check for installed updates, including any failed updates, follow these steps to view the device's update history:

- Open **Settings**
- Navigate to **Update & Security**
- Choose **Windows Update** from the categories in the left navigation
- Choose **View update history**

6.11.4 Reviewing Windows Update logs

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

The Windows Update log files provide administrators with rich information on Windows updates, including failures. The following topic provides an overview of Windows Update log files available, including tools to access and manipulate them.

- Windows Update log files: https://docs.microsoft.com/en-us/windows/deployment/update/windows-update-logs

6.11.5 Installing Windows updates via the command line

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

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 install update packages, see the following articles:

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

6.11.6 Querying for Windows version and hardware information

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

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

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

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

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

6.12 Accessing measurements of the management subsystem

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

Administrators may audit the events listed for FPT_GVI_EXT.1 and FPT_ML_EXT.1 as measurements of the health subsystem. In addition, 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

6.13 Managing audit policy and event logs

Role	Administrator
Windows Editions	Server Standard Server Datacenter Enterprise

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.

The following log locations are always enabled:

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

For additional background on 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, including categories of audits in the Windows Security log: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing

6.13.1 Storing audit data remotely

By default, Windows stores log data on the local machine. Administrators may configure machines to store auditable log data on an external IT entity. The preferred solution for managing log data remotely is a management system such as System Center Operations Manager (SCOM), as described below. In an environment without SCOM or a similar management system, such as in this evaluation, a remote path may be configured on individual devices to store event data on a remote system.

The Log Properties of each log enables a local administrator to configure a remote path to store the log under.

- Establish a trusted channel to the remote log path. A trusted channel must be established via IPsec between the external IT entity receiving off-loaded audit data and the TOE. See the section, Managing IPsec and VPN connections for more information. No additional configuration is required to ensure the audit data transferred from the TOE to the external IT entity is protected by the trusted channel.
- Open the Windows Event Viewer.
- Choose a log from the tree, e.g. the Security log.
- Right-click on the log and choose Properties.
- Set the Log path: to the path on the remote server for the log files.

For more information on the additional properties available for logs, see the following topic:

- Planning and deploying advanced security audit policies: https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/planning-and-deploying-advanced-security-audit-policies#bkmk-4

An example of a system that audit data may be offloaded to is System Center Operations Manager (SCOM). On the SCOM system, the Operations Console is used to configure and view the off-loaded audit events. If the SCOM system is configured to pull the TOE for audit data, then when the local audit data is stored on the TOE it is available to the SCOM system. The link below has information for configuring the SCOM system to pull the audit data from the TOE:

- Operations Manager : https://docs.microsoft.com/en-us/system-center/scom/?view=sc-om-2019

The machine must be joined to a domain where SCOM is configured. The machine must be configured to overwrite the oldest events in the log when new incoming events will exceed the local storage space configured for the given audit log. See the guidance on using the Wevtutil utility below to achieve this.

6.13.2 Managing audit policy with the Auditpol command

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

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

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

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

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

- Logon operations:

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

- Audit policy changes:

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

- IPsec operations:

```
auditpol /set /subcategory:”IPsec Main Mode” /success:enable /failure:enable
auditpol /set /subcategory: “IPsec Quick Mode” /success:enable /failure:enable
```

- Configuring IKEv1 and IKEv2 connection properties:

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

- Registry changes (modifying TLS ciphersuite priority):

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

6.13.3 Managing audit policy with the Secpol snap-in

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

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

6.13.4 Managing audit policy with the Wevtutil utility

Wevtutil is a system utility that performs many of the event auditing management functions including the following:

- Configuring local audit storage capacity, including enabling or disabling automatic log overwriting
- Configuring audit rules, including enabling and disabling optional event logging by feature area
- Configuring log retention policy between automatic overwrite or retain
- Enabling analytic and debug logs (e.g. Microsoft-Windows-CodeIntegrity/Verbose)
- Enumerating log names
- Clearing logs

See the following topic for more information on Wevtutil, including a list of commands:

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

6.13.5 Retrieving and viewing audit logs using the Windows Event Viewer

The Windows Event Viewer may be used to retrieve and view audit logs on a local or remote computer. To launch Event Viewer, follow these steps:

- From the **Start** menu, navigate to **Windows Administrative Tools**.
- Choose **Event Viewer**.
- Use the tree in the left pane to navigate between different Windows, application, and services logs.
- Event Viewer defaults to the Local Computer. To connect to a remote computer that you have administrative rights to, right-click on **Event Viewer (Local)** in the tree and choose **Connect to Another Computer...** .
- To view any Analytic or Debug logs, select the option **Show Analytic and Debug Logs** from the **View** menu.

6.13.6 Retrieving and viewing audit logs using PowerShell

The PowerShell Get-WinEvent cmdlet may be used to retrieve and view audit logs on a local or remote computer. 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

6.13.7 Configuring System Access Control Lists to audit registry changes

In addition to enabling audit policy as noted in the preceding sections, administrators may configure auditing for changes to the Windows registry by changing the audit permissions of the System Access Control List (SACL) for the appropriate registry key folder. For general information on System Access Control Lists, see the following topic:

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

In the evaluated configuration, the following registry key folders have been configured for auditing:

- \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

6.13.7.1 Configuring registry key folder SACLs using the registry editor

The following process describes how to set the SACL for a registry object via the registry editor:

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. everyone or a specific 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

6.13.7.2 Configuring registry key folder SACLs using PowerShell

PowerShell may also be used to set the SACL on a registry key using Powershell. See the following topics for more information:

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

6.13.7.3 Configuring a global SACL for registry changes with Auditpol

The Auditpol command may be used to set a global SACL, for example, to generate auditable events for all registry changes. See the following topic for more information:

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

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 by scenario

The following table lists the set of auditable events in scope for this Common Criteria evaluation, per the selections made in the Security Target. Prerequisite steps are noted for each scenario, for example, setting specific audit policy or enabling specific event log configuration options. For more information on the utilities used to configure audit policy or event logs, see the section Managing audit policy. The table is alphabetized by the Common Criteria requirement related to the event scenario. Reference the subsequent section for the message and field details for each event ID listed in this table.

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
FAU_GEN.1.1	Start-up and shut-down of the audit functions		Security: **4608** (Startup) Security: **1100** (Shut down) *Enable logging of startup and shutdown events with the following command:* ***auditpol /set /subcategory:"Security State Change" /success:enable /failure:enable***
FAU_STG_EXT.1	Failure of audit data capture due to lack of disk space or pre-defined limit. On failure of logging function, capture record of failure and record upon restart of logging function.		Security: **1104** *As specified in the Security Target for this evaluation, logs are configured to overwrite when full and will not fail due to reaching a pre-defined limit. To disable automatic log overwriting, set the log's retention mode to true with wevtutil:* ***wevtutil sl [Log Name] /rt:true***
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session. Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.	System: **36888** (Failure) System: **36880** (Establishment) Microsoft-Windows-SChannel-Events/Perf: **1793** (Terminate) *Enable additional secure channel event logging by changing the registry key value from 1 to 4-7 (see logging options here) in the following registry:* ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL***

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
			Enable logging for Microsoft-Windows-SChannel-Events/Perf using the following command: ***wevtutil sl Microsoft-Windows-Schannel-Events/Perf /e***
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Establishment / Termination of an IPsec SA.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.	Security: **4651, 5451** (Initiation) Security: **4655, 5452** (Termination) Security: **4652, 4654** (Failure) *Enable IPsec events in the Security log:* ***auditpol /set /subcategory:"IPsec Main Mode" /success:enable /failure:enable*** ***auditpol /set /subcategory: "IPsec Quick Mode" /success:enable /failure:enable***
FCS_RBG_EXT.1	Failure of the randomization process.		System: **20**
FCS_TLSC_EXT.2	Failure to establish a TLS Session. Establishment / Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address).	Failure: Windows Logs -> System: **36888** Establishment: Windows Logs -> System: **36880** Terminate: Microsoft-Windows-SChannel-Events/Perf: **1793** *Enable additional secure channel event logging by changing the registry key value from 1 to 4-7 (see logging options here) in the following registry:* ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL***

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
			Enable logging for Microsoft-Windows-SChannel-Events/Perf using the following command: ***wevtutil sl Microsoft-Windows-Schannel-Events/Perf /e***
FCS_TLSS_EXT.2	Failure to establish a TLS Session. Establishment / Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address).	System: **36888** (Failure) System: **36880** (Establishment) Microsoft-Windows-SChannel-Events/Perf: **1793** (Terminate) *Enable additional secure channel event logging by changing the registry key value from 1 to 4-7 (see logging options here) in the following registry:* ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL*** *Enable logging for Microsoft-Windows-SChannel-Events/Perf using the following command:* ***wevtutil sl Microsoft-Windows-Schannel-Events/Perf /e***
FDP_PPR_EXT.1	Successful and failed VM connections to physical devices where connection is governed by configurable policy. Security policy violations.	VM and physical device identifiers. Identifier for the security policy that was violated	Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Networking: **26074** (Success) Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **12140** (Failure, Policy Violation)

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
			Applications and Services Logs\Microsoft\Windows\WMI-Activity\Operational: **5858** (Policy Violation due to Insufficient Privilege) *Enable logging for the Hyper-V-VMMS log with both of the following commands.* ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:false /ca:""*** ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:true /q***
FDP_VNC_EXT.1	Successful and failed attempts to connect VMs to virtual and physical networking components. Security policy violations. Administrator configuration of inter-VM communications channels between VMs.	VM and virtual or physical networking component identifiers. Identifier for the security policy that was violated.	Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **12597, 12598** (Success, Configuration) Security: **4656** (Failure, Policy Violation) Applications and Services Logs\Microsoft\Windows\WMI-Activity\Operational: **5858** (Policy Violation due to Insufficient Privilege)
FIA_UIA_EXT.1	Administrator authentication attempts (all use of the identification and authentication mechanism).	Provided user identity, origin of the attempt (e.g., console, remote IP address).	Security: **4624** (Authentication attempt, successful), **4625** (Authentication attempt, failed) Security: **4624** (Start time) Security: **4634** (End time)

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
	Administrator session start time and end time		
FIA_X509_EXT.1	Failure to validate a certificate.	Reason for failure.	Applications and Services Logs > Microsoft > Windows >CAPI2 > Operational: **11**
FMT_MOF_EXT.1 (#1)	Ability to update the Virtualization System		Setup: **1** (Initiation) Setup: **2** (Success) Setup: **3** (Failure)
FMT_MOF_EXT.1 (#2)	Ability to configure Administrator password policy as defined in FIA_PMG_EXT.1		Security: **4739** *Enable logging for authentication policy change events with the following command:* ***auditpol /set /subcategory:"Authentication Policy Change" /success:enable /failure:enable***
FMT_MOF_EXT.1 (#3)	Ability to create, configure and delete VMs		Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Admin: **13002** (Create)**, 13003** (Delete) Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Analytic: **12170** (Configure, adding components), **12180** (Configure, removing components) Applications and Services Logs\Microsoft\Windows\VHDMP: **12** (Configure, creating virtual disk), **16** (Configure, deleting virtual disk) *Enable logging for the Hyper-V-VMMS log with both of the following commands. Note that if retrieving these*

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
			events through Event Viewer, the View option for Show Analytic and Debug Logs must be enabled. ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:false /ca:""*** ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:true /q***
FMT_MOF_EXT.1 (#4)	Ability to set default initial VM configurations		Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Analytic: **12170** (Configure, adding components), **12180** (Configure, removing components) Applications and Services Logs\Microsoft\Windows\VHDMP: **12** (Configure, creating virtual disk), **16** (Configure, deleting virtual disk) *Enable logging for the Hyper-V-VMMS log with both of the following commands. Note that if retrieving these events through Event Viewer, the View option for Show Analytic and Debug Logs must be enabled.* ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:false /ca:""*** ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:true /q***
FMT_MOF_EXT.1 (#5)	Ability to configure virtual networks including VM		Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Networking: **26000, 26004, 26012, 26016, 26074**

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
			Enable logging for the Hyper-V-VMMS log with both of the following commands. ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:false /ca:""*** ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:true /q***
FMT_MOF_EXT.1 (#6)	Ability to configure and manage the audit system and audit data		Security: **4719** *Enable events for audit policy changes with the following command:* ***auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:enable***
FMT_MOF_EXT.1 (#7)	Ability to configure VM access to physical devices		Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Analytic: **12170, 12180** *Enable logging for the Hyper-V-VMMS log with both of the following commands. Note that if retrieving these events through Event Viewer, the View option for Show Analytic and Debug Logs must be enabled.* ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:false /ca:""*** ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:true /q***
FMT_MOF_EXT.1 (#8)	Ability to configure inter-VM data sharing		Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Admin: **12514**

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
			Enable logging for the Hyper-V-VMMS log with both of the following commands. Note that if retrieving these events through Event Viewer, the View option for Show Analytic and Debug Logs must be enabled. ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:false /ca:""*** ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:true /q***
FMT_MOF_EXT.1 (#9)	Ability to enable/disable VM access to Hypercall functions		**N/A,** as the hypercall interfaces may not be disabled for an enlightened guest operating system.
FMT_MOF_EXT.1 (#10)	Ability to configure removable media policy		Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Analytic: **12170, 12180** *Enable logging for the Hyper-V-VMMS log with both of the following commands. Note that if retrieving these events through Event Viewer, the View option for Show Analytic and Debug Logs must be enabled.* ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:false /ca:""*** ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:true /q***
FMT_MOF_EXT.1 (#11)	Ability to configure the cryptographic functionality		Security: **4657** (TLS) Security: **5449** (IPsec)

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
FMT_MOF_EXT.1 (#12)	Ability to change default authorization factors		Security: **4657** (ObjectValueName: **ScForceOption**) *Enable logging by configuring the SACL for the following registry folder for auditing. See Configuring System Access Control Lists to audit registry keys.* ***\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System***
FMT_MOF_EXT.1 (#13)	Ability to enable/disable screen lock		Security: **4663**
FMT_MOF_EXT.1 (#14)	Ability to configure screen lock inactivity timeout		Security: **4663**
FMT_MOF_EXT.1 (#15)	Ability to configure remote connection inactivity timeout		Security: **4657** (ObjectValueName: **MaxIdleTime**) *Enable logging by configuring the SACL for the following registry folder for auditing. See Configuring System Access Control Lists to audit registry keys.* ***\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\Terminal Services***
FMT_MOF_EXT.1 (#16)	Ability to configure lockout policy for unsuccessful authentication attempts, specifically: timeouts between attempts, limiting number of attempts during a time period		Security: **4739** *Enable logging for authentication policy change events with the following command:* ***auditpol /set /subcategory:"Authentication Policy Change" /success:enable /failure:enable***

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
FMT_MOF_EXT.1 (#17)	Ability to configure name/address of directory server to bind with		System: **3260**
FMT_MOF_EXT.1 (#18)	Ability to configure name/address of audit/logging server to which to send audit/logging records		Security: **4947** *Enable logging for remote event log management with the following command:* ***auditpol /set /subcategory:" MPSSVC Rule-Level Policy Change" /success:enable /failure:enable***
FMT_MOF_EXT.1 (#19)	Ability to configure name/address of network time server		System: **37**
FMT_MOF_EXT.1 (#20)	Ability to configure banner		Security: **4657** (ObjectValueName: **legalnoticecaption** and/or **legalnoticetext**) *Enable logging by configuring the SACL for the following registry folder for auditing. See Configuring System Access Control Lists to audit registry keys.* ***\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System***
FMT_MOF_EXT.1 (#21)	Ability to connect/disconnect removable devices to/from a VM		Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Analytic: **12170** (Connect) Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Analytic: **12180** (Disconnect)

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
			Enable logging for the Hyper-V-VMMS log with both of the following commands. Note that if retrieving these events through Event Viewer, the View option for Show Analytic and Debug Logs must be enabled. ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:false /ca:""*** ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:true /q***
FMT_MOF_EXT.1 (#22)	Ability to start a VM		Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **18500**
FMT_MOF_EXT.1 (#23)	Ability to stop/halt a VM		Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **18502, 18516**
FMT_MOF_EXT.1 (#24)	Ability to checkpoint a VM		Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **18596**
FMT_MOF_EXT.1 (#25)	Ability to suspend a VM		Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **18510**
FMT_MOF_EXT.1 (#26)	Ability to resume a VM		Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **18518**
FPT_GVI_EXT.1	Actions taken due to failed integrity check.		Microsoft-Windows-HostGuardianService-Client/Admin: **2014**

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
			Enable logging for the Hyper-V-VMMS log with both of the following commands. ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:false /ca:""*** ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:true /q***
FPT_HCL_EXT.1	Attempts to access disabled Hypercall interfaces.	Interface for which access was attempted.	**N/A,** as the hypercall interfaces may not be disabled for an enlightened guest operating system.
FPT_ML_EXT.1	Integrity measurements collected	Integrity measurement values	System: **20**
FPT_RDM_EXT.1	Connection/disconnection of removable media or device to/from a VM. Ejection/insertion of removable media or device from/to an already connected VM.	VM Identifier, Removable media/device identifier, event description or identifier (connect/disconnect, ejection/insertion, etc.)	Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Analytic: **12170** (Connect) Applications and Services Logs\Microsoft\Windows\Hyper-V-VMMS\Analytic: **12180** (Disconnect) *Enable logging for the Hyper-V-VMMS log with both of the following commands. Note that if retrieving these events through Event Viewer, the View option for Show Analytic and Debug Logs must be enabled.* ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:false /ca:""*** ***wevtutil sl Microsoft-Windows-Hyper-V-VMMS-Analytic /e:true /q***

Requirement	Scenario(s)	Additional Audit Contents	Log Name: Event ID (Details) ***Prerequisite Steps***
FPT_TUD_EXT.1	Initiation of update. Failure of signature verification.		Setup: **1** (Initiation) Setup: **3** (Failure)
FTP_ITC_EXT.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions	User ID and remote source (IP Address) if feasible.	Security: **4651, 5451** (IPsec Initiation) Security: **4655, 5452** (IPsec Termination) Security: **4652** (Failure, Main Mode)**, 4654** (Failure, Quick Mode) System: **36880** (TLS, HTTPS Initiation) Microsoft-Windows-SChannel-Events/Perf: **1793** (TLS, HTTPS Termination) System: **36888** (TLS, HTTPS Failure) *Enable additional secure channel event logging by changing the registry key value from 1 to 4-7 (see logging options here) in the following registry:* ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL*** *Enable logging for Microsoft-Windows-SChannel-Events/Perf using the following command:* ***wevtutil sl Microsoft-Windows-Schannel-Events/Perf /e***
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	User ID and remote source (IP address) if feasible.	Security: **4651, 5451** (Initiation) Security: **4655, 5452** (Termination) Security: **4652** (Failure, Main Mode)**, 4654** (Failure, Quick Mode)

7.2 Audit event field details

The following table lists the field details for all auditable events in scope for this Common Criteria evaluation, per the selections made in the Security Target. The table is ordered by Event ID. Reference the preceding section for a mapping of Event IDs to Common Criteria scenarios.

Event ID	Log Location	Message	Field Details
1	Windows Logs >Setup	Initiating changes for package	**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>
2	Windows Logs >Setup	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 Logs >Setup	Windows update could not be installed because … "The data is invalid"	**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>
11	Applications and Services Logs > Microsoft >Windows>CAPI2> Operational	For more details for this event, please refer to the "Details" section	**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>

Event ID	Log Location	Message	Field Details
			UserData->CertGetCertificateChain->Result: <Reason for failure of validation>
12	Applications and Services Logs\Microsoft\Windows \VHDMP	Handle for virtual disk <disk name> created successfully. VM ID = <VM ID, Type = <disk type>, Version = <version>, Flags = <flags>, AccessMask = <access mask>, WriteDepth = <write depth>, GetInfoOnly = <true/false>, ReadOnly = <true/false>, HandleContext = <GUID>, VirtualDisk = <GUID>.	**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> **UserData->VmId,VmName**: <VM identifier> **UserData->Device**: <Virtual device identifier>
16	Applications and Services Logs\Microsoft\Windows \VHDMP	Virtual disk object destroyed: <Virtual Disk GUID>	**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> **UserData->VmId,VmName**: <VM identifier> **UserData->Device**: <Virtual device identifier>
20	Windows Logs > System Source: Kernel-Boot	The last shutdown's success status was <LastShutdownGood event data>. The last boot's success was <LastBootGood event data>.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Kernel-Boot]**: <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	Log Location	Message	Field Details
37	Windows Logs > System	The time provider NtpClient is currently receiving valid time data from <NTP server address>.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <type of event> **System->Security[UserID]**: <Subject identifier > **System->EventID,Level:** <Outcome as Success or Failure> **EventData->Data:** <Configuration change>
1100	Windows Logs >Security Subcategory: Security State Change	The event logging service has shut down	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **N/A**: <Subject identifier>
1104	Windows Logs >Security Source: Eventlog	The security log is now full.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <type of event> **System->Security[UserID]**: <Subject identifier > **System->EventID,Level:** <Outcome as Success or Failure>
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>

Event ID	Log Location	Message	Field Details
2014	Microsoft-Windows-HostGuardianService-Client/Admin	The Host Guardian Service Client failed to unwrap a Key Protector on behalf of a calling process. This event will normally correspond to a failure to startup a shielded virtual machine. Consult the description for further details. This could be related to an attestation issue, a Key Protection Server issue, or a network connectivity issue.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <type of event> **System->Computer**: <subject identifier > **System->EventID,Level:** <Outcome as Success or Failure> **Computer:** <Machine Name>
3260	Windows Logs > System	This computer has been successfully joined to domain <Domain Name>.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <type of event> **System->Computer**: <subject identifier > **System->EventID,Level:** <Outcome as Success or Failure> **EventData->Data:** <Configuration change>
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> **EventData -> SubjectUserSid**: <subject identifier > **System->Keywords**: <Outcome as Success or Failure>
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> **EventData -> SubjectUserSid**: <subject identifier > **System->Keywords**: <Outcome as Success or Failure>

Event ID	Log Location	Message	Field Details
			EventData ->LogonType: <type of logon (e.g. interactive)> **EventData ->LogonID**: <unique logon identification> **EventData ->TargetUserName**: <name of enabled account> **EventData ->TargetDomainName**: <domain of enabled account if applicable, otherwise computer> **EventData ->WorkstationName**: <name of computer user logged on> **EventData ->IpAddress**: <IP address of computer logged on>
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> **EventData-> SubjectUserSid**: <subject identifier > **System->Keywords**: <Outcome as Success or Failure> **EventData ->LogonType**: <type of logon (e.g. interactive)> **EventData ->LogonID**: <unique logon identification> **EventData ->TargetUserName**: <name of enabled account> **EventData ->TargetDomainName**: <domain of enabled account if applicable, otherwise computer> **EventData ->WorkstationName**: <name of computer user logged on> **EventData ->IpAddress**: <IP address of computer logged on>
4634	Windows Logs > Security	An account was logged off.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event>

Event ID	Log Location	Message	Field Details
	Subcategory: Logoff		**EventData -> SubjectUserSid**: <subject identifier > **System->Keywords**: <Outcome as Success or Failure>
4651	Windows Logs > Security Subcategory: IPsec Main Mode	Ipsec main mode security association was established. A certificate was used for authentication.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **System->Keywords**: <Outcome as Success or Failure > **EventData->LocalMMPrincipalName**: <Subject identity > **EventData->RemoteMMPrincipalName:** <Remote User ID> **EventData->RemoteAddress**: <User ID, Remote source IP address>
4652	Windows Logs > Security Subcategory: IPsec Main Mode	IPsec main mode negotiation failed	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **EventData->FailureReason**: <Outcome as Success or Failure; reason for failure> **EventData->LocalAddress**: <Subject identity as IP address> **EventData->RemoteAddress**: < Remote source IP address >
4654	Windows Logs > Security Subcategory: IPsec Main Mode	IPsec quick mode negotiation failed	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **EventData->FailureReason**: <Outcome as Success or Failure; reason for failure> **EventData->LocalAddress**: <Subject identity as IP address> **EventData->RemoteAddress**: <User ID, Remote source IP address>

Event ID	Log Location	Message	Field Details
4655	Windows Logs > Security Subcategory: IPsec Main Mode	IPsec main mode security association ended	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **System ->Keywords**: <Outcome as Success or Failure > **EventData->LocalAddress**: <Subject identity as IP address> **N/A**:<User ID> **EventData->RemoteAddress**: <Remote source IP address>
4656	Windows Logs >Security Subcategory: File System and Handle Manipulation	A handle to an object was requested.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **EventData ->SubjectUserSid**: <subject identifier > **System->Keywords**: <Outcome as Success or Failure> **EventData->ObjectName:** <Configuration change>
4657	Windows Logs >Security Subcategory: Registry	A registry value was modified.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **EventData ->SubjectUserSid**: <subject identifier > **System->Keywords**: <Outcome as Success or Failure> **EventData->ObjectName:** <Name of the audited object, e.g. registry key folder.> For FMT_MOF_EXT.1 (#12) and (#20): \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System For FMT_MOF_EXT.1 (#15): \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\Terminal Services

Event ID	Log Location	Message	Field Details
			EventData->ObjectValueName: <Name of the value changed, e.g. registry key.> For FMT_MOF_EXT.1 (#12): ScForceOption For FMT_MOF_EXT.1 (#20): legalnoticecaption and/or legalnoticetext For FMT_MOF_EXT.1 (#15): MaxIdleTime
4663	Windows Logs >Security Subcategory: Registry	An attempt was made to access an object.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **EventData ->SubjectUserSid**: <subject identifier > **System->Keywords**: <Outcome as Success or Failure>
4719	Windows Logs >Security Subcategory: Audit Policy Change	System audit policy was changed.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **EventData ->SubjectUserSid**: <subject identifier > **System->Keywords**: <Outcome as Success or Failure> **EventData -> *:** <Configuration changes>
4739	Windows Logs > Security Subcategory: Authentication Policy Change	Domain Policy was changed.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **EventData -> SubjectUserSid**: <subject identifier > **System->Keywords**: <Outcome as Success or Failure> **EventData -> *:** <Configuration changes>

Event ID	Log Location	Message	Field Details
4947	Windows Logs > Security Subcategory: MPSSVC Rule-Level Policy Change	A change was made to the Windows Firewall exception list. A rule was modified.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **EventData -> SubjectUserSid**: <subject identifier > **System->Keywords**: <Outcome as Success or Failure> **EventData -> *:** <Configuration changes>
5449	Windows Logs > Security Subcategory: Filtering Platform Policy Change	A Windows Filtering Platform provider context has been changed.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **EventData -> SubjectUserSid**: <subject identifier > **System->Keywords**: <Outcome as Success or Failure> **EventData -> *:** <Configuration changes>
5451	Windows Logs > Security Subcategory: IPsec Quick Mode	IPsec quick mode security association was established	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **System ->Keywords**: <Outcome as Success or Failure > **EventData->LocalAddress**: <Subject identity as IP address> **N/A**:<User ID> **EventData->RemoteAddress**: <Remote source IP address>
5452	Windows Logs > Security Subcategory: IPsec Quick Mode	IPsec quick mode security association ended	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **System ->Keywords**: <Outcome as Success or Failure >

Event ID	Log Location	Message	Field Details
			EventData->LocalAddress: <Subject identity as IP address> **N/A**:<User ID> **EventData->RemoteAddress**: <Remote source IP address>
5858	Applications and Services Logs\Microsoft\Windows\WMI-Activity\Operational	Id = <Guid>; ClientMachine = <Machine Name>; User = <User Name>; ClientProcessId = <Process ID>; Component = <Component Name>; Operation = <Attempted Operation Details>; ResultCode = <Result Code>; PossibleCause = <Possible Cause>	**Source =** WMI-Activity **Task Category** = None **Computer** = <Machine Name> **Result Code** = 0x80041003, whenever the WMI filter is accessed without sufficient permission, e.g., a non-admin attempts an admin-only task.
12140	Applications and Services > Microsoft > Windows > Hyper-V-Worker > Admin (Source: Hyper-V-SynthStor)	<Virtual Machine Name> Attachment <Disk Identifier> failed to open because of error: <Error Message> <Error Code (Policy Violation)>. <Virtual machine ID>	**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> **UserData->VmId,VmName**: <VM identifier> **UserData->String:** <Physical device identifier>
12170	Applications and Services Microsoft-Windows-Hyper-V-VMMS/Analytic	Virtual device <Device Id> added to Virtual machine <Virtual machine ID>	**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> **UserData->VmId,VmName**: <VM identifier> **UserData->Device**: <Virtual device identifier>

Event ID	Log Location	Message	Field Details
12180	Applications and Services Microsoft-Windows-Hyper-V-VMMS/Analytic	Virtual device <Device Id> removed from the virtual machine <Virtual machine ID>	**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> **UserData->VmId,VmName**: <VM identifier> **UserData->Device**: <Virtual device identifier>
12514	Applications and Services Microsoft-Windows-Hyper-V-VMMS/Admin	Found a certificate for server authentication. Remote access to virtual machines is now possible.	**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>
12597	Applications and Services > Microsoft > Windows > Hyper-V-Worker > Admin (Source: Hyper-V-SynthNic)	<VM Name> Network Adapter <Virtual Switch ID> Connected to virtual network. <Virtual Machine ID>	**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> **UserData->VmId,VmName**: <VM identifier> **UserData->NicGuid,NicName**: <Networking component identifier>
12598	Applications and Services > Microsoft > Windows > Hyper-V-Worker > Admin (Source: Hyper-V-SynthNic)	<VM Name> Network Adapter <Virtual Switch ID> Disconnected from virtual network. <Virtual Machine ID>	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <type of event> **System->Security[UserID]**: <Subject identifier >

Event ID	Log Location	Message	Field Details
			System->Level: <Outcome as Success or Failure> **UserData->VmId,VmName**: <VM identifier> **UserData->NicGuid,NicName**: <Networking component identifier>
13002	Applications and Services > Microsoft > Windows > Hyper-V-VMMS/ > Admin	A new virtual machine <VM name> was created. (Virtual machine ID <VM ID>)	**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> **System->EventID:** <Configuration change>
13003	Applications and Services > Microsoft > Windows > Hyper-V-VMMS > Admin	The virtual machine <VM Name> was deleted. (Virtual machine ID <VM ID>)	**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> **System->EventID:** <Configuration change>
18500	Applications and Services > Microsoft > Windows > Hyper-V-Worker/Admin	<VM name> started successfully. (Virtual machine ID <VM ID>)	**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> **System->EventID:** <Configuration change>

Event ID	Log Location	Message	Field Details
18502	Applications and Services > Microsoft > Windows > Hyper-V-Worker/Admin	<VM name> was turned off. (Virtual machine ID <VM ID>)	**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> **System->EventID:** <Configuration change>
18510	Applications and Services > Microsoft > Windows > Hyper-V-Worker/Admin	<VM name> saved successfully. (Virtual machine ID <VM ID>)	**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> **System->EventID:** <Configuration change>
18516	Applications and Services > Microsoft > Windows > Hyper-V-Worker/Admin	<VM name> was paused. (Virtual machine ID <VM ID>)	**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> **System->EventID:** <Configuration change>
18518	Applications and Services > Microsoft > Windows > Hyper-V-Worker/Admin	<VM name> was resumed. (Virtual machine ID <VM ID>)	**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>

Event ID	Log Location	Message	Field Details
			System->EventID: <Configuration change>
18596	Applications and Services > Microsoft > Windows > Hyper-V-Worker/Admin	<VM name> was restored successfully. (Virtual machine ID <VM ID>)	**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> **System->EventID:** <Configuration change>
26000	Applications and Services > Microsoft > Windows > Hyper-V-VMMS > Networking	Switch created, name= <switch ID>, friendly name=<switch name>.	**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> **System->EventID:** <Configuration change>
26004	Applications and Services > Microsoft > Windows > Hyper-V-VMMS > Networking	Switch port created, switch name = <switch ID> switch friendly name = <switch name>, port name = <port ID>, port friendly name=<port name>.	**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> **System->EventID:** <Configuration change>
26012	Applications and Services > Microsoft > Windows > Hyper-V-VMMS > Networking	Internal miniport created, name = <miniport ID>, friendly name = <miniport name>, MAC = <MAC address>.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <type of event> **System->Security[UserID]**: <Subject identifier >

Event ID	Log Location	Message	Field Details
			System->Level: <Outcome as Success or Failure> **System->EventID:** <Configuration change>
26016	Applications and Services > Microsoft > Windows > Hyper-V-VMMS > Networking	External ethernet port <port ID> bound.	**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> **System->EventID:** <Configuration change>
26074	Applications and Services > Microsoft > Windows > Hyper-V-VMMS > Networking	Ethernet switch port connected (switch name = <switch name>, port name = <port name>, adapter GUID = <adapter ID>).	**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> **System->EventID:** <Configuration change>
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>
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 >

Event ID	Log Location	Message	Field Details
			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