Microsoft Windows

Common Criteria Evaluation

Microsoft Windows 10

Windows 10 IPsec VPN Client Operational Guidance

Document Information	
Version Number	1.0
Updated On	October 12, 2016

Table of Contents

1 Introduction

This document provides operational guidance information for a Common Criteria evaluation.

This document provides many links to TechNet and other Microsoft resources which often include an “Applies to:” list of operating system versions. For each such link in this document it has been verified that the link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

1.1 Evaluated Windows Editions and Hardware Platforms

This operational guide applys to the following Windows Operating Systems (OS) editions that were tested as part of the evaluated configuration:

- Microsoft Windows 10 Pro Edition (64-bit version)
- Microsoft Windows 10 Enterprise Edition (64-bit version)

As part of the Common Criteria evaluation, the following computers were used for testing during the evaluation:

- Surface Pro 4
- Surface Book

1.2 Configuration

1.2.1 Evaluated Configuration

The Common Criteria evaluation includes a specific configuration of Windows, the “evaluated configuration”. To run Windows deployments using the evaluated configuration follow the deployment steps and apply the security policies and security settings indicated below.

The Security Target section 1.1 describes the security patches that must be included in the evaluated configuration.

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 as described below.

The following Windows help topic has procedures to download Windows 10 installation media as an ISO file for installation and to install the operating system:

- Get Windows 10: https://www.microsoft.com/en-us/software-download/windows10

Bootable media may be created for Windows 10 using the instructions at the following link (see the "I've downloaded an ISO, now what?" topic):

- Software Download : https://www.microsoft.com/en-us/software-download/faq

Windows 10 may be installed using the instructions at the following link (see the "I've created media using the media creation tool, now what do I do?" topic):

- Software Download : https://www.microsoft.com/en-us/software-download/faq

1.2.1.1 Managing User Roles

The evaluated configuration includes two user roles:

- Local Administrator – A user account that is a member of the local Administrators group
- User – A standard user account that is not a member of the local Administrators group

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

The following Technet topic describes how to make a standard user account a member of the local Administrators group:

- Add a member to a local group: https://technet.microsoft.com/en-us/library/cc772524.aspx[1]

The operational guidance includes sections for "Local Administrator Guidance" and "User Guidance" that correspond to the two user roles. In these sections the available security functionality and interfaces, including all security parameters, are indicated as appropriate for each role.

1.2.1.2 Setup Requirements

The following security policies must be applied by an administrator after completing the OOBE in order to fulfil the security objectives for the evaluated configuration:

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

[1] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

The local administrator can configure the above policy by using the Local Group Policy Editor (gpedit.msc). For more information about the Local Group Policy Editor, see the following link:

- Local Group Policy Editor: https://technet.microsoft.com/en-us/library/cc725970(v=ws.11).aspx[2]

To install and maintain the operating system in a secure state the following guidance must be observed:

- Windows 10 must be installed on trusted hardware platforms
- Users must use a separate account that is a member of the local Administrators group to perform the procedures in sections of this document labeled as “Local Administrator Guidance”
- Administators must utilize the guidance included in this document to administer the TOE

1.2.1.3 Management Functions

Management functions are configured locally on the TOE except for SA lifetimes which may be configured on the VPN Gateway. See the Configuring SA Lifetimes section of this document for more information.

1.2.1.4 Mobile Device Management Solutions

Some of the configurations described in this guide are applied to the device through a Mobile Device Management (MDM) solution. The specific steps to perform a configuration through the MDM are solution-specific and are not described in this document. If an MDM solution is being used see MDM solution documentation for detailed configuration actions.

2 Managing Audits

This section contains the following Common Criteria SFRs:

- Audit Data Generation (FAU_GEN.1), Security Audit Event Selection (FAU_SEL.1)

2.1 Audit Events

The **Log: Event Id** column in the tables below specify the Event Id(s) of the audit events as well as the log location for each audit event. Details for each Event Id are specified in **Table 4: Audit Descriptions**. See the guidance in the **Viewing Events** section of this document for information on how to view the events.

The following required audits are described for FAU_GEN.1:

Description	**Log: Event Id**
Start-up and shutdown of the audit functions	Windows Logs/Security: 4608, 1100

[2] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

All administrative actions	<see Table 2 below>
Specifically defined auditable events listed in Table3	<see second table below>

Table 1: FAU_GEN.1 audits

The following table correlates the set of administrative operations described in this document with their associated audits. Section FMT_SMF_EXT.1 has test procedures to produce these audits.

Management Task	Local Administrative Interface	Remote Administrative Interface	Log: Event Id
1. Specify VPN Gateways to use	• PowerShell • User Interface	• Group Policy • MDM	Windows Logs/Security: 5043
2. Specify client credentials to use	• PowerShell • User Interface	• Group Policy • MDM	Windows Logs/Security: 5040
3. Configuration of IKE protocol version(s) used	• PowerShell • User Interface	• Group Policy • MDM	Windows Logs/Security: 5043
4. Configure IKE authentication techniques used	• PowerShell • User Interface	• Group Policy • MDM	Windows Logs/Security: 5040
5. Configure the cryptoperiod for the established session keys. The unit of measure for configuring the cryptoperiod shall be no greater than an hour	• PowerShell	• Group Policy	N/A – The cryptoperiod is configured on the VPN Gateway
6. Configure certificate revocation check	• PowerShell	• Group Policy	Windows Logs/Security: 4950
7. Specify the algorithm suites that may be proposed and accepted during the IPsec exchanges	• PowerShell	• Group Policy	Windows Logs/Security: 5046
8. load X.509v3 certificates used by the security functions in this PP	• PowerShell • User Interface	• Group Policy • MDM	Applications and Services Logs -> Microsoft -> Windows -> CertificateServicesClient-Lifecycle-User -> Operational: 1006
9. Update Windows and to verify the updates	• PowerShell • User Interface	• Not included in this evaluation	Windows Logs/Setup: 1, 2, 3

Table 2: Management Task audits

Requirement	Description	Additional Record Contents	Log: Event Id
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating.	No additional Information.	Windows Logs/Security: 4719

Requirement	Description	Additional Record Contents	Log: Event Id
FCS_CKM.1	Failure of the key generation activity.	No additional Information.	Microsoft-Windows-Crypto-NCrypt/Operational: 4
FCS_IPSEC_EXT.1	Decisions to DISCARD, BYPASS, PROTECT network packets processed by the TOE. Failure to establish an IPsec SA. Establishment/Termination of an IPsec SA.	Presumed identity of source subject. Identity of destination subject. Transport layer protocol, if applicable. Source subject service identifier, if applicable. The entry in the SPD that applied to the decision. Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.	Windows Logs/Security: 5152 Windows Logs/Security: 4652, 4653, 4654 Windows Logs/Security: 4651, 5451, 4655, 5452
FDP_IFC_EXT.1	Failure to establish exclusive tunnel.	No additional information.	Windows Logs -> System: 20
FDP_PSK_EXT.1	Failure of the randomization process.	None.	Not applicable because FIA_PSK_EXT.1.3 does not claim bit-based pre-shared keys
FMT_SMF.1	Success or failure of function.	No additional information.	<see table above>
FIA_X509_EXT.1	Failure to validate X.509v3 certificate.	Reason for failure of validation.	Applications and Services Logs -> Microsoft -> Windows -> CAPI2 -> Operational: 11
FIA_X509_EXT.2	[if one were required] Failure of the path validation of the X.509 certificate	Reason for failure of path validation.	Applications and Services Logs -> Microsoft -> Windows -> CAPI2 -> Operational: 11
FPT_TUD_EXT.1	Initiation of the update. Any failure to verify the integrity of the update..	No additional information.	Windows Logs/Setup: 1, 2, 3
FTP_ITC_EXT.1	All attempts to establish a trusted channel. Detection of modification of channel data.	Identification of the non-TOE endpoint of the channel.	Windows Logs/Security: 4651, 5451, 4655, 5452 Windows Logs/Security: 4960

Table 3: Auditable Events for Security Target Table 7

Id	Log location	Message	Fields
1	Windows Logs -> Setup	Initiating changes for package	Logged: <Date and time of event> PackageIdentifier: <KB package Id> InitialPackageState: Resolved IntendedPackageState: Installed ErrorCode: <success outcome indicated by 0x0>
2	Windows Logs -> Setup	Package was successfully changed to the Installed state	Logged: <Date and time of event> PackageIdentifier: <KB package Id> IntendedPackageState: Installed ErrorCode: <success outcome indicated by 0x0>
3	Windows Logs -> Setup	Windows update could not be installed because … “The data is invalid”	Logged: <Date and time of event> Commandline: <KB package Id> ErrorCode: <install failure indicated by 0x800700D (2147942413)>
4	Microsoft-Windows-Crypto-NCrypt/Operational	Create key operation failed	Logged: <Date and time of event> Provider Name: <Key storage provider name> Key Name: <Unique name for key> Algorithm Name: <Key algorithm name>
11	Applications and Services Logs -> Microsoft -> Windows -> CAPI2 -> Operational	Build Chain	System/TimeCreated/SystemTime: <Date and time of event> UserData/CertGetCertificateChain/Certificate/subjectName: <subject name in client certificate> UserData/CertGetCertificateChain/CertificateChain/ChainElement/Certificate <issuer of leaf certificate as subject name in chained certificate> TrustStatus -> ErrorStatus: <Error code[3]>
20	Windows Logs -> System Source: Kernel-Boot	The last boot’s success was <LastBootGood event data>.	Logged: <Date and time of event> LastBootGood: <Outcome as true or false indicating if the kernel-mode cryptographic self-tests and RNG initialization succeeded or failed>

[3] Error 20 indicates an untrusted root in the certificate chain.

24	Windows Logs -> System Source: TPM	The Trusted Platform Module (TPM) status: <enabled state> and <active state>.	Logged: <Date and time of event>
400	Applications and Services Logs -> Microsoft -> Windows -> AppXDeployment-Server -> Microsoft-Windows-AppXDeployment-Server/Operational	Deployment Add operation on Package <package Id> from: (<.appx pathname>) finished successfully	Logged: <Date and time of event> User ID: <SID of user account that installed the app> PackageFullName: <package Id> Path: <.appx pathname>
404	Applications and Services Logs -> Microsoft -> Windows -> AppXDeployment-Server -> Microsoft-Windows-AppXDeployment-Server/Operational	AppX Deployment operation failed for package <app package identity> with error <error code>. The specific error text for this failure is: <failure text>.	Logged: <Date and time of event> User ID: <SID of user account that installed the app> PackageFullName: <package Id>
1006	Applications and Services Logs -> Microsoft -> Windows -> CertificateServicesClient-Lifecycle-User -> Operational Applications and Services Logs -> Microsoft -> Windows -> CertificateServicesClient-Lifecycle-System -> Operational	A new certificate has been installed.	Logged: <Date and time of event> Subject: <Certificate subject name, CN, etc.> Thumbprint: <Certificate thumbprint>
1100	Windows Logs -> Security Subcategory: Security State Change	The event logging service has shut down	Logged: <Date and time of event> Keywords: <Outcome as Success>
4608	Windows Logs -> Security Subcategory: Security State Change	Startup of audit functions	Logged: <Date and time of event> Task category: <type of event> 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.	Logged: <Date and time of event> Task category: <type of event> Local Endpoint: <Subject identity as IP address> Remote Endpoint: <Subject identity as IP address of non-TOE endpoint of connection >

			Keying Module Name: <Transport layer protocol as IKEv1 or IKEv2> Local Certificate: <The entry in the SPD that applied to the decision as certificate SHA Thumbprint> Remote Certificate: <The entry in the SPD that applied to the decision as certificate SHA Thumbprint> Cryptographic Information: <The entry in the SPD that applied to the decision as MM SA Id and cryptographic parameters established in the SA> Keywords: <Outcome as Success>
4652, 4653	IPsec Main Mode	IPsec main mode negotiation failed	Logged: <Date and time of event> Task category: <type of event> Local Endpoint: <Subject identity as IP address> Remote Endpoint: <Subject identity as IP address of non-TOE endpoint of connection/channel> Keying Module Name: <Transport layer protocol as IKEv1 or IKEv2> Failure Information: <Outcome as Failure; Reason for failure asthe entry in the SPD that applied to the decision> Cryptographic Information: <The entry in the SPD that applied to the decision as cryptographic parameters attempted to establish in the SA>
4654	IPsec Quick Mode	IPsec quick mode negotiation failed	Logged: <Date and time of event> Task category: <type of event> Local Endpoint: <Subject identity as IP address/port> Remote Endpoint: <Subject identity as IP address/port of non-TOE endpoint of connection/channel > Keying Module Name: <Transport layer protocol as IKEv1 or IKEv2>Failure Information: <Outcome as Failure; Reason for failure as the entry in the SPD that applied to the decision as the MA SA Id, QM Filter Id, Tunnel Id, Traffic Selector Id >
4655	Windows Logs -> Security Subcategory: IPsec Main Mode	IPsec main mode security association ended	Logged: <Date and time of event> Task category: <type of event> Local Endpoint: <Subject identity as IP address/port > Remote Endpoint: <Subject identity as IP address/port of non-TOE endpoint of connection/channel > Keying Module Name: <Transport layer protocol as IKEv1 or IKEv2> Keywords: <Outcome as Success>

4719	Windows Logs -> Security Subcategory: Audit Policy Change	System audit policy was changed	Logged: <Date and time of event> Task category: <category of audit> Task Subcategory: <subcategory of audit> Subcategory GUID: <subcategory GUID name> Security ID: <user identity> Account Name: <account name> Account Domain: <account domain> Login ID: <login Id> Changes: <Success/Failure changes> Keywords: <Outcome as Success or Failure>
4950	Windows Logs -> Security Subcategory: MPSSVC Rule-Level Policy Change	A Windows Firewall setting has changed.	Logged: <Date and time of event> Security ID: <SID of user configuring the setting> Value: <new configuration setting value>
4960	Windows Logs -> Security Subcategory: IPsec Driver	IPsec dropped an inbound packet that failed an integrity check	Logged: <Date and time of event> Task category: <type of event> Cryptographic Parameters <Identification of the non-TOE endpoint of the channel as IP address/port and security parameter index> Keywords: <Outcome as Failure>
5040	Windows Logs -> Security Subcategory: Filtering Platform Policy Change	A change was made to IPsec settings. An authentication set was added.	Logged: <Date and time of event> Task category: <type of event> Keywords: <Outcome as Failure>
5043	Windows Logs -> Security Subcategory: Filtering Platform Policy Change	A change was made to IPsec settings. A connection security rule was added.	Logged: <Date and time of event> Task category: <type of event> Keywords: <Outcome as Failure>
5046	Windows Logs -> Security Subcategory: Filtering Platform Policy Change	A change was made to IPsec settings. A crypto set was added.	Logged: <Date and time of event> Task category: <type of event> Keywords: <Outcome as Failure>
5152	Filtering Platform Packet Drop	The Windows Filtering Platform has blocked a packet.	Logged: <Date and time of event> Process ID: <process ID holding the network connection>

			Account Name: <name of the process holding the network connection > Direction: <Inbound or Outbound> Source Address: <source IP address of source> Source Port: <source port number> Destination Address: <destination IP address> Destination Port: <destination port number> Protocol: <protocol number> Filter Run-Time ID: <Filter ID associated with firewall rule triggering flow denial>
5446	Windows Logs -> Security Subcategory: Filtering Platform Policy Change	Windows Filtering Platform callout has been changed	Logged: <Date and time of event> Task category: <type of event> Change type: <Operation as add, change or delete> Callout ID: <Callout identifier as GUID> Callout Name: <Callout identifier as text-based name> Layer ID: <Layer identifier as GUID> Layer Name: <Layer identifier as text-based name> Keywords: <Outcome as Success or Failure>
5447	Windows Logs -> Security Subcategory: Other Policy Change Events	Windows Filtering Platform filter has been changed	Logged: <Date and time of event> Task category: <type of event> Change type: <Operation as add, change or delete> Filter ID: <Filter Id as GUID> Filter Name: <Filter identifier as text-based name> Layer ID: <Layer Id as GUID> Layer Name: <Layer identifier as text-based name> Additional Information: <Filter conditions>
5450	Windows Logs -> Security Subcategory: Filtering Platform Policy Change	Windows Filtering Platform sub-layer has been changed	Logged: <Date and time of event> Task category: <type of event> Change type: <Operation as add, change or delete> Sub-layer ID: <Sub-layer Id as GUID> Sub-layer Name: <Sub-layer identifier as text-based name>
5451	Windows Logs -> Security Subcategory: IPsec Quick Mode	IPsec quick mode security association was established	Logged: <Date and time of event> Task category: <type of event> Local Endpoint: <Subject identity as IP address/port> Remote Endpoint: <Subject identity as IP address/port of non-TOE endpoint of connection > Keying Module Name: <Transport layer protocol as IKEv1 or IKEv2>

			Cryptographic Information: <The entry in the SPD that applied to the decision as MM SA Id, QM SA Id, Inbound SPI, Outbound SPI and cryptographic parameters established in the SA > Keywords: <Outcome as Success>
5452	Windows Logs -> Security Subcategory: IPsec Quick Mode	IPsec quick mode security association ended	Logged: <Date and time of event> Task category: <type of event> Local Endpoint: <Subject identity as IP address/port> Remote Endpoint: <Subject identity as IP address/port of non-TOE endpoint of connection > Cryptographic Information: <The entry in the SPD that applied to the decision as the QM SA Id, Tunnel Id, Traffic Selector Id> Keywords: <Outcome as Success>

Table 4: Audit Descriptions

{**FAU_GEN.1:A:1**}{**FAU_SEL.1:A:1**}{**FAU_SEL.1:A:2**}{**FAU_SEL.1:A:3**}

2.2 Managing Audit Policy

2.2.1 Local Administrator Guidance

The following log locations are always enabled:

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

The following TechNet topic describes the categories of audits in the Windows Logs -> Security log:

- Advanced Audit Policy Configuration: http://technet.microsoft.com/en-us/library/jj852202(v=ws.10).aspx[4]

The following TechNet topic describes how to select audit policies by category, user and audit success or failure in the Windows Logs -> Security log:

- Auditpol set: https://technet.microsoft.com/en-us/library/cc755264.aspx[5]

[4] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

[5] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

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:

- 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

2.2.1.1 Viewing Events

To view event logs, see the following link:

- Get-EventLog: http://technet.microsoft.com/en-us/library/hh849834.aspx[6]

3 RAS IPsec VPN Client Configuration

This section provides information on how to configure the RAS IPsec VPN Client for IKEv1 and IKEv2 in tunnel mode.

{**FCS_IPSEC_EXT.1:A:2**}{**FTP_ITC.1:A:1**}

3.1 Add a VPN Connection

This section contains the guidance to meet the following Common Criteria SFRs:

- FMT_SMF.1 – Specify VPN Gateways to use
- FMT_SMF.1 – Specify client credentials to use
- FMT_SMF.1 – Configuration of IKE protocol versions

[6] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

The following section describes the configuration of a new connection to the VPN Gateway. Configuring Windows to require all traffic to route through the IPsec tunnel may be done by creating Firewall rules that prevent all traffic that is not routed through the VPN or by using a Lockdown VPN connection deployed through an MDM. For information on how to set Firewall rules see the Managing the Windows Firewall section of this document. Configuring an MDM to deploying VPN connections is out of scope of this guidance.

3.1.1 IT Administrator Guidance

VPN profiles can be managed on Windows 10 using an MDM. See MDM documentation for more information.

3.1.2 Windows 10

1. Go to **Settings -> Network & Internet -> VPN**

2. Click on **Add a VPN connection**

3. Choose the **Windows (built in)** VPN provider

4. Enter the **Connection name** as a text string and enter the **Server name or address** as a DNS name or an IP address

5. Select the **VPN type** as follows:

    1) **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)** – This choice provides an IKEv1 connection

    2) **IKEv2** – This choice provides and IKEv2 connection

6. Configure user credentials as appropriate

The Subject name of the server’s certificate must match the DNS name or IP address entered in the Connection name textbox.

3.2 Configuring Pre-Shared Key for IKEv1

This section contains the guidance to meet the following Common Criteria SFRs:

- Internet Protocol Security (IPsec) Communications (FCS_IPSEC_EXT.1.12) – Pre-shared keys
- FMT_SMF.1 – Configure IKE authentication techniques

The pre-shared key is generated out of band and provided to the client for configuration.

Note: the secret value for the preshared key must be a text-based value manually entered as shown in the **Key** editbox in the **Advanced Properties** dialog below. The secret value must match the secret value configured on the VPN server. While the secret can be any length, it should include at least 22 characters and up to 10000 characters as determined at the discretion of the administrator. For example organizational policies can enforce the use of strong passwords containing a minimum number of characters using at least one upper and one lower case letter, one number, and one special character from among the following: ! @ # $ % ^ & * ().

{**FCS_IPSEC_EXT.1:A:9**}{**FCS_IPSEC_EXT.1:A:10**}{**FIA_PSK_EXT.1:A:1**}{**FIA_PSK_EXT.1:A:2**}

3.2.1 Windows 10

1. Go to **Settings -> Network & Wireless -> VPN**
2. Click on an existing VPN connection or add a new VPN connection
3. Choose the **Windows (built in)** VPN provider
4. Enter the **Connection name** as a text string and enter the **Server name or address** as a DNS name or an IP address
5. For the VPN type select L2TP/IPsec with pre-shared key
6. Enter the pre-shared key that was received out of band from the VPN Gateway{**FIA_PSK_EXT.1:A:3**}

3.3 Configuring Connections to Use Certificates

This section contains the guidance to meet the following Common Criteria SFRs:

- Internet Protocol Security (IPsec) Communications (FCS_IPSEC_EXT.1)
- FMT_SMF.1 – Configure IKE authentication techniques

3.3.1 Configuring Certificate Authentication for IKEv1

3.3.1.1 Windows 10

1. Right click the network icon in the lower right corner of the task bar and click **Open Network and Sharing Center**
2. On the **Nework and Sharing Center** page click **Change adapter settings**
3. On the **Network connections** page right-click **VPN Connection** and then click P**roperties** to open the **VPN Connections Properties** dialog

4. On the Properties page go to the **Security** tab and under **Authentication** select the **Use machine certificates** radio button.
5. Click the **OK** button.

3.3.2 Configuring Certificate Authentication for IKEv2

3.3.2.1 Windows 10

1. Right click the network icon in the lower right corner of the task bar and click **Open Network and Sharing Center**
2. On the **Nework and Sharing Center** page click **Change adapter settings**
3. On the **Network connections** page right-click **VPN Connection** and then click P**roperties** to open the **VPN Connections Properties** dialog
4. On the Properties page go to the **Security** tab and under **Authentication** select the **Use machine certificates** radio button.
5. Click the **OK** button.

3.4 Configuring Cryptographic Algorithms

3.4.1 Configuring the Cryptographic Algorithms for IKEv1 and IKEv2

This section contains the guidance to meet the following Common Criteria SFRs:

- FMT_SMF.1 - Specify the algorithm suites that may be proposed and accepted during the IPsec exchanges

The Set-VpnConnectionIpsecConfiguration PowerShell cmdlet is used to configure the algorithms used:

- Set-VpnConnectionIpsecConfiguration : https://technet.microsoft.com/en-us/library/dn262642(v=wps.630).aspx[7]

  The EncryptionMethod option is used to set the main mode encryption algorithm.

  The CipherTransformationConstants option is used to set the quick mode encryption algorithm.

[7] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

In order to prevent security being reduced while transitioning from IKE Phase 1 / IKEv2 SA, an authorized administrator must configure the IPsec VPN client such that the algorithms are the same strength for both phases of IKE. For example, if EncryptionMethod is set to use AES256 then the CipherTransformationConstant option must be set to either AES256 or AESGCM256 and the hashing algorithms of the two phases must also be the same strength.

{FCS_IPSEC_EXT.1:A:4}{FCS_IPSEC_EXT.1:A:6}

3.5 Configuring the Client Lifetimes

This section contains the guidance to meet the following Common Criteria SFRs:

- Internet Protocol Security (IPsec) Communications (FCS_IPSEC_EXT.1.8)
- FMT_SMF.1 - Configure the cryptoperiod for the established session keys

Lifetime settings for tunnel mode using the RAS IPsec VPN interface for IKEv1 and IKEv2 are configured on the VPN gateway. Clients configured for transport mode may configure client lifetime settings by following the instructions in the section Configuring SA Lifetimes.

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.

3.6 Connecting to the VPN Gateway

The following sections provide instructions on how to connect to the VPN gateway **using the** VPN client.

{**FDP_IFC_EXT.1:A:1**}

3.6.1 Windows 10

1. Go to **Settings -> Network & Internet -> VPN**

2. Click on the VPN Connection and then click the **Connect** button

Note: After clicking the Connect button the user may be prompted for credentials in some cases.

3.7 Other Information

There is no way to configure Windows to use IKEv1 aggressive mode. Only main mode is supported.

{**FCS_IPSEC_EXT.1:A:7**}

4 IPsec Configuration with Transport Mode

The following link provides information on configuring IPsec in transport mode:

- Securing End-to-End IPsec Connections by Using IKEv2 in Windows Server 2012 : http://technet.microsoft.com/en-us/library/hh831807.aspx[8]

{**FCS_IPSEC_EXT.1:A:2**}

4.1 Supported Algorithms

The following table lists the supported DH Groups:

DH Groups	PowerShell Value
DH Groups 14 (2048-bit MODP)	DH14
DH Group 19 (256-bit Random ECP)	DH19
DH Group 20 (384-bit Random ECP)	DH20

The following table lists the supported symmetric encryption algorithms:

[8] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

Symmetric Encryption	PowerShell Value
AES-CBC-128	AES128
AES-CBC-256	AES256
AES-GCM-128 (only supported in quick mode)	AESGCM128
AES-GCM-256 (only supported in quick mode)	AESGCM256

Note that AES-GCM-128 and AES-GCM-256 may only be configured for quick mode. In addition, when AES-GCM-128 is configured then the hashing algorithm must be AES-GMAC-128 and when AES-GCM-256 is configured the hashing algorithm must be AES-GMAC-256.

The following table lists the supported hashing algorithms:

Hashing Algorithm	PowerShell Value
SHA-1	SHA1
SHA-256	SHA256
SHA-384	SHA384
AES-GMAC-128 (only supported in quick mode)	AESGMAC128
AES-GMAC-256 (only supported in quick mode)	AESGMAC256

Care must be taken to ensure that the cryptographic algorithm configuration specifies a main mode encryption algorithm that is at least as strong as the quick mode algorithm.

4.2 Configuring Cryptographic Algorithms

This section contains the guidance to meet the following Common Criteria SFRs:

- FMT_SMF.1 - Specify the algorithm suites that may be proposed and accepted during the IPsec exchanges

Main mode cryptographic algorithms are configured with the New-NetIPsecMainModeCryptoProposal PowerShell cmdlet:

- New-NetIPsecMainModeCryptoProposal : https://technet.microsoft.com/en-us/library/jj573824(v=wps.630).aspx[9]

[9] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

Quick mode cryptographic algorithms are configured with the New-NetIPsecQuickModeCryptoProposal PowerShell cmdlet:

- New-NetIPsecQuickModeCryptoProposal : https://technet.microsoft.com/en-us/library/jj554875(v=wps.630).aspx[10]

The Encryption option used with the New-NetIPsecQuickModeCryptoProposal cmdlet must NOT be set to a stronger encryption algorithm than the Encryption option used with the New-NetIPsecMainModeCryptoProposal cmdlet. The Encryption option used with the New-NetIPsecMainModeCryptoProposal cmdlet must always be equivalent or stronger than the Encryption option used with the New-NetIPsecQuickModeCryptoProposal cmdlet.

In order to prevent security being reduced while transitioning from IKE Phase 1 / IKEv2 SA, an authorized administrator must configure the rules such that the algorithms are the same strength for both phases of IKE. The algorithm specified for the Encryption option used with New-NetIPsecMainModeCryptoProposal must be the same as the algorithm specified for the Encryption option used with New-NetIPsecQuickModeCryptoProposal. The hash options must also be the same.

{**FCS_IPSEC_EXT.1:A:4**}{**FCS_IPSEC_EXT.1:A:6**}

4.3 Configuring SA Lifetimes

This section contains the guidance to meet the following Common Criteria SFRs:

- Internet Protocol Security (IPsec) Communications (FCS_IPSEC_EXT.1.8)
- FMT_SMF.1 - Configure the cryptoperiod for the established session keys

This section provides instructions on how to configure SA lifetime values. SA lifetimes are configured both locally and remotely on the VPN Gateway. When using transport mode SA lifetimes are configured locally and when using tunnel mode SA lifetimes are configured on the VPN Gateway. The configuration of the VPN Gateway is out of scope of this guidance.

{**FCS_IPSEC_EXT.1:A:8**}

4.3.1 Configuring Main Mode SA Lifetimes

The Set-NetIpsecMainModeCryptoSet PowerShell cmdlet is used to configure the main mode SA lifetime:

- Set-NetIPsecMainModeCryptoSet : https://technet.microsoft.com/en-us/library/jj554872(v=wps.630).aspx[11]

[10] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

[11] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

See the section on MaxMinutes

4.3.2 Configuring Quick Mode SA Lifetimes

The New-NetIpsecQuickModeCryptoProposal PowerShell cmdlet is used to configure the quick mode SA lifetime:

- New-NetIpsecQuickModeCryptoProposal : https://technet.microsoft.com/en-us/library/jj554875(v=wps.630).aspx[12]

  See the sections on MaxKiloBytes and MaxMinutes

4.4 Configuring Signature Algorithms

This section contains the guidance to meet the following Common Criteria SFRs:

- FMT_SMF.1 – Specify client credentials to use

The following table lists the signature algorithms that are supported for IPsec authentication with certificates.

Signature Algorithms
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:

- New-NetIpsecAuthProposal : https://technet.microsoft.com/en-us/library/jj554847(v=wps.630).aspx[13]

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. See the documentation at the link above for information on what values are acceptable for the SubjectNameType option. In order to support an IP address in the remote entity's certificate, the remote entity's certificate Subject name may be a Common Name (CN) with the IP address as the value of the Common Name. In addition, the RemoteAddress and SubjectName options for the New-NetIpsecAuthProposal cmdlet must be set to the IP address in the certificate.

{**FCS_IPSEC_EXT.1:A:11**}

[12] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.
[13] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

4.5 Configuring the IKEv1 or IKEv2 Protocol in the IPsec Rule

This section contains the guidance to meet the following Common Criteria SFRs:

- FMT_SMF.1 – Configuration of IKE protocol versions

When configuring transport mode connections the protocol type is configured using the KeyModule parameter switch with the New-NetIpsecRule PowerShell cmdlet:

- New-NetIpsecRule : https://technet.microsoft.com/en-us/library/jj554889(v=wps.630).aspx[14]

5 Managing the Windows Firewall (Windows Filtering Platform)

This section contains the guidance to meet the following Common Criteria SFRs:

- Internet Protocol Security (IPsec) Communications (FCS_IPSEC_EXT.1.1)

The Windows Filtering Platform is configured to start automatically and must never be turned off in order to support any of the described IPsec scenarios. The Windows Filtering Platform is the IPsec Security Policy Database (SPD) for Windows 10. The IPsec rules in the Windows Filtering Platform are entries in the SPD.

The Windows Filtering Platform can be configured to use Inbound and Outbound rules that PROTECT, BYPASS, DISCARD and ALLOW traffic specified by the Inbound and Outbound rules. An overview

- Overview of Windows Firewall with Advanced Security: https://technet.microsoft.com/en-us/library/dd448535(v=ws.10).aspx[15]

The following TechNet topic provides a step by step guide for configuring the Windows Firewall and IPsec Policy:

- Windows Firewall and IPsec Policy Deployment Step-by-Step Guide: https://technet.microsoft.com/en-us/library/deploy-ipsec-firewall-policies-step-by-step(v=ws.10).aspx[16]

The following TechNet topic explains the priority for applying firewall rules:

[14] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

[15] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

[16] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

- Understanding the Firewall: http://technet.microsoft.com/en-us/library/dd421709(v=ws.10).aspx[17]

In particular, the topic above notes that “Block connection” rules have higher priority than “Allow connection” rules (where “Block connection” is equivalent to DISCARD and “Allow connection” is equivalent to ALLOW). Further, it says that the “Default profile behavior” when the Windows Filtering Platform is turned on (which is mandatory for IPSEC configuration) explicitly DISCARDs all network traffic that is not specified as ALLOWed by the combination of the IPSEC rules as well as Inbound and Outbound Firewall rules. The Windows Filtering Platform in this way implements the final catch-all denial SPD entry.

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

- Network Security Cmdlets in Windows PowerShell: https://technet.microsoft.com/en-us/library/jj554906(v=wps.630).aspx[18]

{FCS_IPSEC_EXT.1:A:1}{FCS_IPSEC_EXT.1:A:3}

6 Managing Certificates

This section contains the guidance to meet the following Common Criteria SFRs:

- Internet Protocol Security (IPsec) Communications (FCS_IPSEC_EXT.1.12) – Trusted root certificates
- FMT_SMF.1 - Load X.509v3 certificates

{FCS_IPSEC_EXT.1:A:12}{FIA_X509_EXT.2:A:1}

6.1 IT Administrator Guidance

Root certificates can be added to and removed from Windows 10 using an MDM. See MDM documentation for more information.

6.1.1 Local Administrator Guidance

On Windows 10 authentication certificates are obtained through MDM, domain policy or manually.

The following TechNet topic describes managing certificates (including the “Obtain a Certificate” sub-topic):

[17] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

[18] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

- Manage Certificates : http://technet.microsoft.com/en-us/library/cc771377.aspx[19]
- Certutil: http://technet.microsoft.com/library/cc732443.aspx[20]

The following TechNet topic describes how to delete a certificate:

- Delete a Certificate: http://technet.microsoft.com/en-us/library/cc772354.aspx[21]

7 Managing Certificate Validation

This section contains the guidance to meet the following Common Criteria SFRs:

- Extended: X.509 Certificate Validation (FIA_X509_EXT.1)
- Extended: X.509 Certificate Use and Management (FIA_X509_EXT.2)
- FMT_SMF.1 - Configure certificate revocation check

Windows 10 performs certificate validation by default when using IPsec with certificates. No configuration is necessary to cause the certificate validation to be performed. In order to configure Windows 10 to require revocation checking the following configuration is necessary.

The following PowerShell cmdlet is used to require certificate revocation checking:

```
Set-NetFirewallSetting -CertValidationLevel RequireCrlCheck
```

- Set-NetFirewallSetting : http://technet.microsoft.com/en-us/library/jj554878.aspx[22]

{**FIA_X509_EXT.1:A:1**}{**FIA_X509_EXT.1:A:2**}{**FIA_X509_EXT.2:A:2**}

8 Managing Random Number Generation

This section contains the guidance to meet the following Common Criteria SFRs:

[19] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

[20] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

[21] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

[22] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

- Extended: Cryptographic Operation (Random Bit Generation) (FCS_RBG_EXT)

No configuration is needed for random number generation on Windows 10.

9 Traversing a NAT

Windows 10 automatically traverses a NAT as specified in the IKEv1 and IKEv2 protocols and the SAs are negotiated. No configuration is necessary to accommodate a NAT in a deployment.

{**FCS_IPSEC_EXT.1:A:5**}

10 Recovering an Interrupted Connection

If network connectivity is interrupted, then the established SA remains in use until either the SA lifetime limits or the configured network outage time is exceeded. If network connectivity is re-established within these the two timeframes, then the established SA will continue to function on the re-established network connection.

In the tunnel mode case the user if the connection is dropped then the user will need to connect again.

In the case of transport mode a if the connection is dropped a new SA will be negotiated when traffic resumes.

11 Managing Updates

This section contains the guidance to meet the following Common Criteria SFRs:

- Extended: Trusted Update (FPT_TUD_EXT.1)
- FMT_SMF.1 - Update Windows and to verify the updates

For Windows 10, Windows Update is described in the following technet articles:

- Keep your PC up to date: http://windows.microsoft.com/en-us/windows/windows-update

The following steps shall be performed in order to check for updates for Windows 10:

- Open **Settings**
- Click **Update & Security**

- Under Windows Update, click **Check for updates**

The local administrator configures automatic updates as described in the following TechNet topic:

- Configure Automatic Updates using Group Policy: https://technet.microsoft.com/en-us/library/dd939933.aspx[23]

Updates to Windows are delivered as Microsoft Update Standalone Package files (.msu files) and are signed by Microsoft.

The Windows operating system will check that the signature and certificate is valid and if not then the update will not be installed.

{**FPT_TUP_EXT.1:A:1**}

12 Protection of the TSF

This section contains the guidance to meet the following Common Criteria SFRs:

- Extended: TSF Self Test (FPT_TST_EXT)

Windows executable files are protected by the mechanisms listed below:

- All Windows Update packages are signed.
- Windows Code Integrity verifies signatures on all kernel mode device drivers.
- Windows Code Integrity verifies signatures on key OS user mode binaries.
- An administrator may check the file integrity for all Windows executable files using the sfc.exe utility.

Windows Code Integrity will generate events as specified in the “Auditing for Cryptographic Operations” section of this document if a binary signature does not verify. However, if a signature fails to verify that is critical for the system to log audits then the audit will not be generated, in this case the operating system will not boot.

The sfc.exe utility must be run in an elevated command window. The following is an example command to verify the Windows binary bcrypt.dll.

[23] The content in this link applies to Microsoft Windows 10 Pro Edition and Microsoft Windows 10 Enterprise Edition.

```
sfc.exe –verifyfile=c:\windows\system32\bcrypt.dll
```

The success or failure of the integrity check when using the sfc utility is displayed in the output of the utility.

{**FPT_TST_EXT.1:A:1**}{**FPT_TST_EXT.1:A:2**}