Microsoft Windows

Common Criteria Evaluation

Microsoft Windows 10

Microsoft Windows Server 2016

Microsoft Windows Server 2012 R2

Windows 10, Server 2016, and Server 2012 R2 Server Virtualization Operational Guidance

Document Information	
Version Number	.61
Updated On	October 30, 2017

TABLE OF CONTENTS

1 Introduction

This document provides the Operational Guidance for the Certification Authority Common Criteria Evaluation according to the Assurance Activity requirements reflected in the protection profile.

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 the Windows Operating System (OS) versions listed in the following section.

1.1 Evaluated Windows Editions and Hardware Platforms

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

- Microsoft Windows Server 2016
- Microsoft Windows Server 2016 Datacenter edition
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012 R2 Datacenter edition
- Microsoft Windows 10 Enterprise Edition (64-bit version)

As part of the Common Criteria evaluation, the following hardware platforms were tested as part of the evaluated configuration:

- Microsoft Surface Book
- Dell OptiPlex 3040
- HP ProDesk 600 G2

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 also be installed from installation media as described below.

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

- Create Windows 10 Installation Media: https://www.microsoft.com/en-us/software-download/windows10

The following topic has procedures to download Windows Server 2016 and Windows Server 2012 R2 installation media as an ISO file that may be used for either the Standard or DataCenter editions, depending upon the licensing information that is provided during installation (choose the "Evaluated Now" menu item):

- Windows Server Evaluations: https://www.microsoft.com/en-us/evalcenter

Windows Server 2016 may be installed using the instructions at the following link:

- Windows Server 2016: https://technet.microsoft.com/en-us/windows-server-docs/get-started/windows-server-2016

Windows Server 2012 R2 may be installed using the instructions at the following link:

- Installing Windows Server 2012: http://technet.microsoft.com/en-us/library/jj134246.aspx

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. For Local Administrator role, no additional measures are needed to control access to the user-accessible functions in a secure processing environment. A standard user may be allowed to Start, Checkpoint and Suspend VMs by adding the user to the **Hyper-V Administrators** group. The following TechNet topics describe how to add a user to a group:

- Add a member to local group : https://technet.microsoft.com/en-us/library/cc772524(v=ws.11).aspx

The operational guidance includes instructions for members of the Local Administrators group to manage the TOE. Standard user accounts who are a member of **Hyper-V Administrators** group cannot manage the TOE aside from configuring the screen lock interval on virtualization server and having the ability to manage virtual machines. **{FMT_MOF_EXT.1:G:1}. {FMT_MOF_EXT.1:G:2)**

1.2.1.2 Setup Requirements

Configure the following security policy settings:

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

2 Manage Audits (FAU)

2.1 Managing Audit Policy

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

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

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

- Configuring the Windows Firewall
  auditpol /set /subcategory:"MPSSVC Rule-Level Policy Change" /success:enable /failure:enable

- Configuring the Logon Banner:
- Configuring TLS Cipher Suite priority:
  auditpol /set /subcategory:"Registry" /success:enable /failure:enable
  reg add HKLM\Software\Policies\Microsoft\Cryptography\Configuration\SSL\00010002\CC

  In addition to enabling audit policy as noted above, each registry key to be audited must also have its auditing permissions enabled. This is done as follows:

  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) 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

  The following is the list of registry keys that must be audited:

  - (Logon Banner) HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Policies/System
  - (TLS Cipher Suite Priority) HKEY_LOCAL_MACHINE /Software/Policies/Microsoft/Cryptography/Configuration/SSL/00010002

To enable/disable event logging in the Application and Services Logs, see the following link describing how to enumerate the log names and set the enabled state of the log:

- Wevtutil: http://technet.microsoft.com/en-us/library/cc732848.aspx

Schannel success audits for initiating a trusted channel are configured as described by the following Microsoft Support topic:

- How to enable Schannel event logging: https://support.microsoft.com/en-us/kb/260729

Schannel success audits for termination of the trusted channel are configured by enabling logging for Microsoft-Windows-SChannel-Events/Perf using the following command:

- wevtutil sl Microsoft-Windows-Schannel-Events/Perf /e

The authorized local administrator may review the audit log by use of the **Get-EventLog** PowerShell cmdlet. The following TechNet topic describes the syntax for using this cmdlet and also includes several examples demonstrating how to extract individual information from the audit records in order to verify that all records expected have been generated and that the audit records contain the expected information:

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

The authorized local administrator may review events from event logs, including classic logs, such as the System and Application logs, the event logs that are generated by the Windows Event Log technology and log files generated by Event Tracing for Windows (ETW) by use of the **Get-WinEvent** PowerShell cmdlet. The following MSDN page describes the syntax for using this cmdlet and also includes several examples:

- Get-WinEvent: https://msdn.microsoft.com/en-us/powershell/reference/5.0/microsoft.powershell.diagnostics/get-winevent

The Event Viewer administrator tool also provides a mechanism to review the audit trail as described in this TechNet topic that also includes information on creating custom views that filter the audit trail according to various criteria based on the individual information in the audit records:

- Event Viewer How To…: http://technet.microsoft.com/en-us/library/cc749408.aspx

2.2 Read Audit Records

This section contains the following SFRs:
FAU_SAR.1 Audit Review

The authorized local administrator may review the audit log by use of the Get-EventLog PowerShell cmdlet. The following TechNet topic describes the syntax for using this cmdlet and also includes several examples demonstrating how to extract individual information from the audit records in order to verify that all records expected have been generated and that the audit records contain the expected information:

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

The Event Viewer administrator tool also provides a mechanism to review the audit trail as described in this TechNet topic that also includes information on creating custom views that filter the audit trail according to various criteria based on the individual information in the audit records:

- Event Viewer How To: http://technet.microsoft.com/en-us/library/cc749408.aspx

2.3 Audit Data Generation

The following required audit events are described for FAU_GEN.1:

Table 1 below describes the set of audit events required by the security target for operation of the Server Virtualization security functions. **Table 2** describes the set of audit events associated with the administrative commands to configure manage the TOE security functionality. **Table 3** specifies the format of the audit events described by Tables 1 and 2.

Table 1: Required Auditable Events

SFR	Auditable Events	Additional Audit Record Contents	Log: Event Id
FAU_GEN.1	Startup and shutdown of audit functions		Windows Logs\Security: **1100**, **4608**
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.	None	**N/A:** not applicable based on the ST selecting overwriting oldest events with newest events when log fills
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.	Failure: Windows Logs -> System: **36888** Establishment: Windows Logs -> System: **36880** Terminate: Microsoft-Windows-SChannel-Events/Perf: **1793**
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Establishment/Termination of an IPsec SA.	Reason for failure.	Initiation: Windows Logs\Security:**4651, 5451**

		Non-TOE endpoint of connection (IP address) for both successes and failures.	Termination: Windows Logs\Security:**4655, 5452** Failure: Windows Logs\Security:**4652, 4653, 4654**
FCS_RBG_EXT.1	Failure of the randomization process.	No additional information.	Windows Logs -> System: **20**
FCS_TLSC_EXT.1	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**
FCS_TLSS_EXT.1	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**
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 Microsoft-Windows-Hyper-V-VMMS/Analytic: **12170** (Success) Applications and Services Logs\Microsoft\Windows\Hyper-V-SynthStor\Admin: **12140** (Failure, Policy Violation)
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.	Failure, Policy Violation: Windows Logs\Security: **4656** <u>Windows Server 2012 R2:</u> Success, Configuration : Applications and Services Logs\Microsoft\Windows\Hyper-V-SynthNic\Admin: **12597** <u>Windows 10 Enterprise / Windows Server 2016:</u> Success, Configuration : Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **12597**

FTP_TRP.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.	Initiation: Windows Logs\Security:**4651, 5451** Termination: Windows Logs\Security:**4655, 5452** Failure: Windows Logs\Security:**4652, 4653, 4654**
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).	Windows Logs\Security: **4624, 4625**
	Administrator session start time and end time.	None.	Start time: Windows Logs\Security: **4624** End time: Windows Logs\Security: **4634**
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	Updates to the TOE. Configuration changes (system, network, audit function, Guest VM time, etc.). Start-up and shutdown of the TOE VM Start/Stop/Suspend events. Start and end of remote management session.	Configuration changes.	Updates to the TOE: Windows Logs->Setup: **1, 2, 3** Configuration changes: see **Table 2** Start-up and shutdown of the TOE: Windows Logs\Security: **1100**, **4608** VM Start/Stop/Suspend events: Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **18500, 18502, 18504, 18510** Start and end of remote management session: Windows Logs\Security: **4624, 4634**
	Account created, modified, enabled, disabled, removed,	None.	Create: Windows Logs\Security: **4720** Modify: Windows Logs\Security: **4738** Enable: Windows Logs\Security: **4722** Disable: Windows Logs\Security: **4725** Remove: Windows Logs\Security: **4726**
FPT_TUD_EXT.1	Initiation of update.	No additional information.	Initiation: Windows Logs/Setup: **1**

	Failure of signature verification.		Failure: Windows Logs/Setup: **3**
FPT_HCL_EXT.1	Attempts to access disabled hypercall interfaces. Security policy violations.	Interface for which access was attempted. Identifier for the security policy that was violated.	**N/A**: Hypecall functions may not be disabled.
FPT_RDM_EXT.1	Transfer of removable media or device between VMs.	None.	Applications and Services Microsoft-Windows-Hyper-V-VMMS/Analytic: **12170** (Success)

Table 2: Administrative Audit Events

FMT_MOF_EXT.1.1

Administrative Action/Management Functions	Log: Event Id
1. Ability to administer the Virtualization System locally and remotely;	Windows Logs/Security: **4624, 4625**
2. Ability to update the Virtualization System, and to verify the updates using [**digital signature**] capability prior to installing those updates;	Windows Logs/Setup: **1, 2, 3**
3. Ability to configure password policy [Minimum password length, Minimum password complexity, Maximum password lifetime]	Windows Logs/Security: **4739**
4. Ability to create, delete, and configure VMs;	Create, Delete : Applications and Services Microsoft-Windows-Hyper-V-VMMS/Admin: **13002, 13003** Configure : Applications and Services Microsoft-Windows-Hyper-V-VMMS/Analytic: **12170, 12180**
~~5. Ability to set default initial VM configurations;~~	N/A
6. Ability to configure virtual networks including VMs;	Applications and Services Microsoft-Windows-Hyper-V-VMMS/Networking: **26000, 26004, 26012, 26016, 26074**
7. Ability to manage the audit system and audit data;	Windows Logs/Security: **4719**

8. Ability to configure VM access to physical devices;		Applications and Services Microsoft-Windows-Hyper-V-VMMS/Analytic: **12170, 12180**
9. Ability to configure inter-VM data sharing;		Applications and Services Microsoft-Windows-Hyper-V-VMMS/Admin: **12514**
10. Ability to enable/disable VM access to Hypercall functions;		
11. Ability to configure removable media policy;		Applications and Services Microsoft-Windows-Hyper-V-VMMS/Analytic: **12170, 12180**
12. [selection:]	***Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1***	Windows Logs/Security: **4657**
	Ability to configure the cryptographic functionality	TLS: Windows Logs/Security: **4657** IPsec: Windows Logs/Security: **5449**
	~~Ability to change default authorization factors~~	N/A
	Ability to enable/disable screen lock	Windows Logs/Security: **4663**
	Ability to configure screen lock inactivity timeout	Windows Logs/Security: **4663**
	Ability to configure remote connection inactivity timeout	Windows Logs/Security: **4663**
	Ability to configure lockout policy for unsuccessful authentication attempts through limiting number of attempts during a time period	Windows Logs/Security: **4739**
	Ability to configure name/address of directory server to bind with	Windows Logs/System: **3260**
	Ability to configure name/address of audit/logging server to which to send audit/logging records	Windows Logs/Security: **4947**
	Ability to configure name/address of network time server	Windows Logs/System: **37**
	Ability to configure advisory warning message in banner, as described in FTA_TAB.1	Windows Logs/Security: **4657**

	Ability to enable/disable password authentication.	Windows Logs/Security: **4662**

FMT_MOF_EXT.1.2

Administrative Action/Management Functions	Log: Event Id
Ability to connect/disconnect removeable devices to/from a VM	Connect : Applications and Services Microsoft-Windows-Hyper-V-VMMS/Analytic: **12170** Disconnect : Applications and Services Microsoft-Windows-Hyper-V-VMMS/Analytic: **12180**
Ability to start a VM	Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **18500**
Ability to checkpoint a VM	Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **18596**
Ability to suspend a VM	Applications and Services Logs\Microsoft\Windows\Hyper-V-Worker\Admin: **18510**

Table 3: Audit Event Details

Note: The fields in the following table refer to the hierarchical field names used in event Details Friendly View (Details tab, Friendly View radio button selected). The field names also correspond to the node names in XML files provided as evidence. The Message correspond to the message displayed in the General event view (General tab).

Id	Log location	Message	Fields
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> **UserData->CertGetCertificateChain->Result**: <Reason for failure of validation>
20	**Windows Logs -> System**	The last boot's success was <LastBootGood event data>.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <type of event> **System-> Security[UserID]**: <subject identifier > **EventData->LastBootGood**: <Outcome as true or false indicating if the kernel-mode cryptographic self-tests and RNG initialization succeeded or failed>
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>
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>
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>
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>
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> **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** Subcategory: Logoff	An account was logged off.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <type of event> **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 >
4653	**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**: <User ID, 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>
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:** <Requested file>
4662	**Windows Logs->Security** Subcategory: Other Object Access Events	An operation was performed on 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> **EventData->ObjectName:** <Configuration change>
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>
4720	**Windows Logs->Security** Subcategory: User Account Management	A user account was created.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4722	**Windows Logs->Security** Subcategory: User Account Management	A user account was enabled.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4725	**Windows Logs->Security** Subcategory: User Account Management	A user account was disabled.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
4726	**Windows Logs->Security**	A user account was deleted.	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure>

	Subcategory: User Account Management		**EventData->SubjectUserSid**: <Subject identifier>
4738	**Windows Logs->Security** Subcategory: User Account Management	A user account was changed	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Task**: <Type of event> **System->Keywords**: <Outcome as Success or Failure> **EventData->SubjectUserSid**: <Subject identifier>
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>
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>
5447	**Windows Logs -> Security** Subcategory: Other Policy Change Events	A Windows Filtering Platform filter 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>
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 > **EventData->LocalAddress**: <Subject identity as IP address> **N/A**:<User ID> **EventData->RemoteAddress**: <Remote source IP address>
12140	Windows Server 2012 R2: **Applications and Services -> Microsoft -> Windows -> Hyper-V-SynthStor -> Admin** Windows Server 2016: **Applications and Services -> Microsoft -> Windows -> Hyper-V-Worker -> Admin** (Source: Hyper-V-SynthStor)	Attachment <disk identifier> failed to open because of error: <Error Message> <ErrorCode>. <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>
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	Windows Server 2012 R2: **Applications and Services -> Microsoft -> Windows -> Hyper-V-SynthNic -> Admin** Windows Server 2016:	<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>

	Applications and Services -> Microsoft -> Windows -> Hyper-V-Worker -> Admin (Source: Hyper-V-SynthNic)		**UserData->NicGuid,NicName**: <Networking component identifier>
12670	Windows Server 2012 R2: **Applications and Services -> Microsoft -> Windows -> Hyper-V-SynthNic -> Admin** Windows Server 2016: **Applications and Services -> Microsoft -> Windows -> Hyper-V-Worker -> Admin** (Source: Hyper-V-SynthNic)	<VM Name> failed to allocate resources while connecting to a virtual network: Insufficient system resources exist to complete the requested service. (<Error Code>) (Virtual Machine ID <Virtual Machine ID>). The Ethernet switch may not exist.	**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:** <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>
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>
18504	**Applications and Services -> Microsoft -> Windows -> Hyper-V-Worker/Admin**	<VM name> was shut down using the Shutdown Integration Component with parameters: Force = false, Reason = 'Shutdown	**System->TimeCreated**[**SystemTime**]: <Date and time of event> **System->Provider[Name]**: <type of event> **System->Security[UserID]**: <Subject identifier >

		initiated by <Username> using Hyper-V management tools.' (Virtual machine ID <VM ID>)	**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>
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 > **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>

<table>
<tr><td></td><td></td><td></td><td>System->EventID: <Configuration change></td></tr>
<tr><td>26074</td><td>Applications and Services -> Microsoft -> Windows -> Hyper-V-VMMS -> Networking</td><td>Ethernet switch port connected (switch name = <switch name>, port name = <port name>, adapter GUID = <adapter ID>).</td><td>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></td></tr>
<tr><td>36880</td><td>Windows Logs -> System</td><td>An TLS server handshake completed successfully. The negotiated cryptographic parameters are as follows:</td><td>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></td></tr>
<tr><td>36888</td><td>Windows Logs -> System</td><td>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.</td><td>System->TimeCreated[SystemTime]: <Date and time of event>
System->Provider[Name]: <type of event>
System->Security[UserID]: <subject identifier >
<u>Windows Server 2016:</u>
UserData->EventXML->TargetName: <Non-TOE endpoint >
UserData->EventXML->AlertDesc: < Reason for failure>
UserData->EventXML->ErrorState: < Reason for failure >
<u>Windows Server 2012 R2:</u>
EventData->AlertDesc: < Reason for failure >
EventData->ErrorState: < Reason for failure >

The following are the possible error codes:
Description — Error Code Value
Unexpected message — 10
Bad record MAC — 20
Record overflow — 22
Decompression fail — 30
Handshake failure — 40
Illegal parameter — 47
Unknown CA — 48
Access denied — 49
Decode error — 50
Decrypt error — 51
Protocol version — 70
Insufficient security — 71
Internal error — 80</td></tr>
</table>

			Unsupported extension	110

2.4 Off-Loading Audit Data

{FAU_STG_EXT.1:G:1}. {FAU_STG_EXT.1:G:2}

Audit data may be off-loaded to an external IT entiry.

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://technet.microsoft.com/en-us/library/hh205987(v=sc.12).aspx

The TOE must be joined to a domain where SCOM is configured. The TOE 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. The following TechNet topic describes how to configure audit log retention policy (see the /rt: <Retention> parameter in the link below):

Wevtutil: http://technet.microsoft.com/en-us/library/cc732848.aspx

A trusted channel must be established between the external IT entity receiving off-loaded audit data and the TOE as described in section “Manage IPsec (FCS)”. 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.

3 Manage Protection Mechanisms (FDP)

3.1 Manage Inter-VM Data Sharing

Hyper-V supports the following mechanisms for sharing data between host and virtual machine and between virtual machines:

- Virtual Networking
- Host drives
- Clipboard

Drives and clipboard inter-VM data sharing is configured using Virtual Connection Manager (VMConnect). For more information see https://technet.microsoft.com/en-us/library/dn282274.aspx.

VMConnect is turned off by default on Windows Server 2012 R2.

3.2 Manage Physical Platform Resources

{FDP_PPR_EXT.1:G:1}. {FDP_PPR_EXT.1:G:2}. {FDP_PPR_EXT.1:G:3}. {FPT_RDM_EXT.1:G:1}. {FMT_MOF_EXT.1}

By default a Guest VM is denied access to all physical platform resources on the host. The Hyper-V manager provides settings for an administrator to configure access by a Guest OS to physical platform resources on the host.

To add a physical hard disk for direct access by a Guest VM see Add-VMHardDiskDrive (see "Example 4").
To configure a physical hard disk that is directly accessible by a Guest VM see Set-VMHardDiskDrive.
To remove a physical hard disk from direct access by a Guest VM see Remove-VMHardDiskDrive.
Note: the physical hard disk device may be removable media (e.g. an inserted USB drive).

To add a physical DVD drive for direct access by a Guest VM see Add-VMDvdDrive.
To configure a physical DVD drive that is directly accessible by a Guest VM see Set-VMDvdDrive.
To remove a physical DVD drive from direct access by a Guest VM see Remove-VMDvdDrive.

To configure a physical network adapter for direct access by a virtual switch for direct access by a Guest VM through its virtual network adapter see section Manage Virtual Networking.

3.3 Manage Virtual Networking

{FDP_VNC_EXT.1:G:1}. {FMT_MOF_EXT.1:G:1}

The following technet article describes virtual networking: http://social.technet.microsoft.com/wiki/contents/articles/11524.windows-server-2012-hyper-v-network-virtualization-survival-guide.aspx

Hyper-V Virtual Switch Overview: https://technet.microsoft.com/en-us/library/hh831823.aspx

3.4 Manage Hardware-Based Isolation

{FDP_HBI_EXT.1:G:1)

The following TechNet topic describes system requirements in the UEFI for Hyper-V:

- System requirements for Hyper-V on Windows Server 2016: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/system-requirements-for-hyper-v-on-windows[i]

4 Manage Trusted Communication Channels (FTP)

4.1 Manage Remote Administration

Hyper-V Supports three methods of remote administration:

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

Remote Administrators must logon the remote administration interfaces using TOE administrator credentials in order to remotely perform the Management Functions listed in Table 2.

For more information on deploying and managing Remote Desktop Services on the Hyper-V host, see https://technet.microsoft.com/library/ff710446(ws.10).aspx.

For more information on using Hyper-V manager see https://technet.microsoft.com/en-us/library/cc770494.aspx.

For more information on using Hyper-V Powershell commands, see Hyper-V Cmdlets.

All methods of remote administration are secured using IPsec as described in Managing IPsec or using TLS or TLS/HTTPS as described in Managing TLS.

4.2 Manage User Interface

{FTA_UIF_EXT.1:G:1}

Each VM connection is displayed in a separate window on the Windows desktop. The window with input focus also is drawn in the foreground in front of all other Windows.

The Hyper-V VM Manager assigns each VM with a unique nameThe Hyper-V administrator must use this name, or the DNS name of the guest VM, when managing guest VMs using the Hyper-V Microsoft Management Console (MMC) snap-in.

5 Manage IPsec (FCS)

{FCS_IPSEC_EXT.1:G:1}, {FCS_IPSEC_EXT.1:G:2}, {FCS_IPSEC_EXT.1:G:3}, {FCS_IPSEC_EXT.1:G:4}, {FCS_IPSEC_EXT.1:G:5}, {FCS_IPSEC_EXT.1:G:6}, {FCS_IPSEC_EXT.1:G:7}, {FCS_IPSEC_EXT.1:G:9}, {FCS_IPSEC_EXT.1:G:10}, {FCS_IPSEC_EXT.1:G:11}, {FCS_IPSEC_EXT.1:G:12}, {FCS_IPSEC_EXT.1:G:13}, {FCS_IPSEC_EXT.1:G:14}

IPsec is used to provide a trusted communication channel between the TOE and the remote administrator.

For guidance on establishing the trusted communication channel using an IPsec policy the administrator may refer to the "Microsoft Windows 10 IPsec VPN Client" operational guidance documentation and the "Windows 10 (Anniversary Update) and Windows Server 2016 IPsec VPN Client" operational guidance documentation in the Common Criteria Deployment and Administration section of the following link:

- Windows Platform Common Criteria Certification : https://msdn.microsoft.com/en-us/library/dd229319.aspx

The Windows Firewall is used to configure the Network Flow Control Policy in order to allow specific types of network traffic between endpoints that need not be authenticated. Firewall Rules allow or block network traffic based on various criteria. The TOE then processes allowed network traffic. For example a rule allowing ICMP network protocol traffic results in the TOE processing that traffic according to the ICMP standard. Connection Security Rules configure the authentication of two computers before they begin communications using the IPsec protocol. The TOE then processes IKE traffic to authenticate the two computers according to the IKE protocol. The following two TechNet topics explain the Windows Firewall Rules and Connection Security Rules in more detail:

- Understanding Firewall Rules: http://technet.microsoft.com/en-us/library/dd421709(v=ws.10).aspx
- Understanding Connection Security Rules: http://technet.microsoft.com/en-us/library/dd448591(v=ws.10).aspx

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.

5.1 IPsec 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
DH Group 24 (2048-bit MODP with 256-bit POS)	DH24

The following table lists the supported symmetric encryption algorithms:

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

6 Managing Identification and Authentication (FIA)

6.1 Manage Passwords

{FIA_PMG_EXT.2:G:1} {FIA_PMG_EXT.2:G:1}

The following TechNet topics describe the characteristics for strong passwords and best practices and how to establish security policies for minimum password length and complexity:

- Password must meet complexity requirements: https://technet.microsoft.com/en-us/library/hh994562(v=ws.10).aspx
- Password must meet complexity requirements: https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/password-must-meet-complexity-requirements
- Passwords Technical Overview (see the Strong Passwords section): https://technet.microsoft.com/en-us/library/hh994558(v=ws.10).aspx
- Minimum password length: https://docs.microsoft.com/en-us/windows/device-security/security-policy-settings/minimum-password-length

The following TechNet topic describes how administartors manage password authentication:

- Net user: https://technet.microsoft.com/en-us/library/bb490718.aspx

Windows Domain settings allow accounts to be configured to allow logon only with a smartcard. This setting is performed on a Domain Controller and is outside the scope of the TOE.

6.2 Logon

{**FIA_UIA_EXT.2:G:1**}, {**FIA_UIA_EXT.2:G:2**}

The following TechNet topic describes how administrators conduct interactive logon with a user name and password and verify their administrator account status:

- How do I log on as an administrator?: http://windows.microsoft.com/en-US/windows7/How-do-I-log-on-as-an-administrator

In domain environments the IT admin may configure logon with a smart card or a virtual smart card. In this case an administrator may logon a domain-joined TOE using their smart card or virtual smart card by typing CTRL-ALT-DELETE and providing the correct PIN associated with the smart card or virtual smart card. If the IT admin configures multiple authentication methods, then the “Sign-in options” link is displayed at logon for the administrator to choose which authentication method to utilize. The domain-joined TOE does not require additional configuration for smart card authentication.

The following TechNet link provides describes configuring virtual smart card authentication on the TOE in steps 2 and 3 (note step 1 must first be performed on a Domain Controller and is outside the scope of the TOE):

- Get Started with Virtual Smart Cards: Walkthrough Guide: https://technet.microsoft.com/en-us/library/dn579260(v=ws.11).aspx

6.3 Manage Lockout

{FMT_MOF_EXT.1:G:1}

The following TechNet topic explains the net accounts command line utility for managing password length and lifetime:

- 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 for managing account lockout policy:

/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. {**AGD1: FIA_AFL_EXT.1}**

/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.

6.4 Manage X.509 Certificate Validation

{**FIA_X509_EXT.1:G:1**}

The following TechNet topic describes how to configure Windows to not establish an IPsec trusted channel if certificate validation fails, or if Windows is not able to check the validation status for a certificate:

- Set-NetFirewallSetting: https://technet.microsoft.com/en-us/library/jj554878(v=wps.630).aspx (see RequireCRLCheck)

By default Windows will will inform the user and seek their consent before establishing a HTTPS web browsing session channel if certificate validation fails, or if Windows is not able to check the validation status for a certificate.

6.5 Manage X.509 Certificate Authentication

{**FIA_X509_EXT.2:G:2**}

Certificate authentication configuration is performed as described in Managing IPsec and Managing TLS.

7 Administer the TOE (FMT)

7.1 Restrict Security Roles

{**FMT_SMR.2:G:1**}

See Management Functions for information on managing the TOE locally. See Manage Remote Administration for information on managing the TOE remotely.

7.2 Configure Data Sharing

See Manage Inter-VM Data Sharing

7.3 Restrict Administration of Hyper-V

{FPT_INT_EXT.1:G:1}

Only an authorized administrator may perform the management functions described in this section.

7.4 Management Functions

Management Functions	Guidance for each Management Function
1. Ability to administer the Virtualization System locally and remotely;	See Manage Remote Administration for remote administration
2. Ability to update the Virtualization System, and to verify the updates using [digital signature] capability prior to installing those updates;	See Update the Virtualization System
3. Ability to configure password policy o Minimum password length, o Minimum password complexity, o Maximum password lifetime.	See Manage Passwords
4. Ability to create, delete, and configure VMs;	See New Virtual Machine Wizard and Virtual Machine Settings
5. Ability to set default initial VM configurations;	There are no configurable default settings for new VMs
6. Ability to configure virtual networks including VMs;	See Manage Virtual Networking
7. Ability to manage the audit system and audit data;	See Managing Audits
8. Ability to configure VM access to physical devices;	See Manage Hardware-Based Isolation and Manage Physical Platform Resources
9. Ability to configure inter-VM data sharing;	See Manage Inter-VM Data Sharing
10. Ability to enable/disable VM access to Hypercall functions;	VM access to hypercall functions can be prevented by using an unenlightened guest OS
11. Ability to configure removable media policy;	See Manage Physical Platform Resources
12. Configure Hyper-V Security	See Managing Identification and Authentication
Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1	See Managing Logon Banner
Ability to configure the cryptographic functionality	See Manage IPsec (FCS) and Managing TLS
Ability to change default authorization factors	See Manage Passwords
Ability to enable/disable screen lock	See Security Policy Settings Overview: http://technet.microsoft.com/en-us/library/2fdcbb11-8037-45b1-9015-665393268e36 Note: section “Interactive logon: Machine inactivity limit”
Ability to configure screen lock inactivity timeout	Same as above
Ability to configure remote connection inactivity timeout	For Remote Desktop Services inactivity timeout limits see Session Time Limits: https://technet.microsoft.com/en-us/library/ee791886(v=ws.10).aspx

	For inactivity timeout limits for remote administration using Hyper-V Manager and PowerShell the inactivity timeout is set on the remote machine in the same way as specified for the **Ability to configure screen lock inactivity timeout** management function above.
Ability to configure lockout policy for unsuccessful authentication attempts through [limiting number of attempts during a time period]	See Manage Lockout
Ability to configure name/address of directory server to bind with	See How to Join Your Computer to a Domain: https://technet.microsoft.com/en-us/library/bb456990.aspx Note: the directory server name/address is provided by your IT admin
Ability to configure name/address of audit/logging server to which to send audit/logging records	See Off-Loading Audit Data
Ability to configure name/address of network time server	See Windows Time Service Tools and Settings: https://technet.microsoft.com/en-us/library/cc773263(v=WS.10).aspx
Ability to configure advisory warning message in banner, as described in FTA_TAB.1	See Managing Logon Banner
Ability to enable/disable password authentication.	See Manage Passwords
Ability to connect/disconnect removeable devices to/from a VM	See Get-Disk and Add-VMHardDiskDrive
Ability to start a VM	See Start VM
Ability to checkpoint a VM	See Checkpoint-VM
Ability to suspend a VM	See Suspend-VM

In addition to the guidance above for creating new VMs, each VM should be given a unique name. A process for creating unique names for guest VMs follows:

1) Create the VM using a descriptive name
2) After the VM is created, run the following PowerShell command:

   Get-VM <vmname> | ft VMId

3) Rename the newly created VM using the pattern <vmname>-<vmid> and the VMId obtained in the previous step.

7.5 Management and Operational Networks

As described in the section Manage Remote Administration, there are three methods for remote administration. The following mechanisms all provide the ability to cryptographically, logically, or physically separate the management network and the operational network:

- IPsec – see Manage IPsec (FCS)
- TLS, TLS/HTTPS – see Managing TLS
- Logical means – see Manage Virtual Networking
- Physical means – see Manage Virtual Networking (for example Hyper-V Manager may configure a separate virtual switch for each physical network adapter on the Hyper-V host)

Note that the IPSEC and the TLS-based mechanisms can be layered with each other, and also with logical and physical separation mechanisms. The mechanisms described above are typically not mutually exclusive.

8 Protecting the Virtualization System (FPT)

8.1 Update the Virtualization System

To determine the operating system version go to Control Panel -> System and Security -> System.

System updates are obtained through Windows Update as described by the following TechNet topic:

- What is Windows Update?: http://windows.microsoft.com/en-us/windows/windows-update

System updates may be run by a standard user when executed through the Windows Update process. System updates may also be applied by administrators by the Windows Update Standalone Installer as described by the following Microsoft Support topic:

- Description of the Windows Update Standalone Installer in Windows: http://support.microsoft.com/en-us/kb/934307

The following Windows topic describes how to determine the system information. The successfully installed updates are indicated in the generated listing under the label “Hotfixes:”, including a count and listing of all the system updates that have been installed enumerated by the Knowledge Base designation (e.g. KB3002885) designation associated with the updates:

- Systeminfo: http://technet.microsoft.com/en-us/library/cc771190.aspx

Certificates used to verify system updates are not configurable and not managed. **{FPT_TUD_EXT.1:G:1}**

8.2 Hypercall Controls

Hypercall interfaces supported by Hyper-V are described in Hypervisor Specifications: https://msdn.microsoft.com/en-us/virtualization/hyperv_on_windows/develop/tlfs?f=255&MSPPError=-2147217396. Refer to the versions v4.0b and v5.0b[1] of the specification. **{FPT_HCL_EXT.1:G:1}**

8.3 Removable Devices

See Manage Physical Platform Resources.

9 Managing TLS

{**FCS_TLSS_EXT.1:G:1**}, {**FCS_TLSS_EXT.1:G:2**}, {**FCS_TLSS_EXT.1:G:3**}

TLS cipher suite selection and priority may be configured on the server side of a connection.

The DN in the certificate is automatically compared to the expected DN and does not require additional configuration of the expected DN for the connection.

The mandatory and optional cipher suites listed in the Security Target correlate with those available in the TOE as follows:

Table 4: Selected TLS Cipher Suites

Cipher Suites (per Security Target)	Cipher Suite Requirement	Available Cipher Suites in TOE[2]
TLS_RSA_WITH_AES_128_CBC_SHA	Mandatory	TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA	Optional	TLS_RSA_WITH_AES_256_CBC_SHA
~~TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246~~	Optional	Not supported
~~TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246~~	Optional	Not supported
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492	Optional	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256 or TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492	Optional	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256 or TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492	Optional	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256 and/or

[1] Note the v5.0b spec applies to both Windows 10 and Windows Server 2016
[2] See: Cipher Suites in Schannel: http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757(v=vs.85).aspx

		TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492		TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256 and/or TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246	Optional	TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246	Optional	TLS_RSA_WITH_AES_256_CBC_SHA256
~~TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246~~	Optional	Not supported
~~TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246~~	Optional	Not supported
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289	Optional	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289	Optional	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289	Optional	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289	Optional	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384

The following MSDN article describes how the administrator modifies the set of TLS cipher suites for priority and availability:

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

The following MSDN article describes how the administrator modifies the settings to limit protocol availability. The TOE must be configured to disable the SSL 1.0, SSL 2.0, SSL 3.0 and TLS 1.0 protocols.

- TLS/SSL Settings: https://technet.microsoft.com/en-us/library/dn579260(v=ws.11).aspx

The DN in the certificate is automatically compared to the expected DN and does not require additional configuration of the expected DN for the connection.

The TOE comes preloaded with root certificates for various Certificate Authorities. The following TechNet topic describes how to manage trust relationships:

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

Hashes in the TLS protocol are configured in association with cipher suite selection. The administrator configures the cipher suites used on a machine by following the configuration instructions at the following link: http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757(v=vs.85).aspx

In Windows 10 and Windows Server 2016 an elliptic curve priority order setting is supported so the elliptic curve suffix is not required and is overridden by the new elliptic curve priority order, when provided, to allow organizations to use group policy to configure different versions of Windows with the same cipher suites.

- TLS Cipher Suites in Windows 10 v1607: https://msdn.microsoft.com/en-us/library/windows/desktop/mt490158(v=vs.85).aspx

In Windows Server 2012 R2, cipher suite strings were appended with the elliptic curve to determine the curve priority.

- TLS Cipher Suites in Windows 8.1: https://msdn.microsoft.com/en-us/library/windows/desktop/mt767781(v=vs.85).aspx

The reference identifier in the TOE for TLS is the URL of the server. There is no configuration of the reference identifier.

The signature algorithm is not configurable in the TOE.

9.1 Manage TLS Mutual Authentication

{**FCS_TLSS_EXT.1:G:4**}, {**FCS_TLSS_EXT.1:G:5**}

See the technet article at https://technet.microsoft.com/en-us/library/hh831709.aspx for information on how to configure IIS to require client certificates during the TLS handshake.

IIS supports different mechanisms for TLS mutual authentication based on the available infrastructure.

For an environment with Active Directory and/or Microsoft Enterprise Certificate Authority, see http://www.iis.net/configreference/system.webserver/security/authentication/clientcertificatemappingauthentication. Additional information on configuring the environment for Active Directory Certificate mapping can be found in this article: https://blogs.msdn.microsoft.com/friis/2017/01/16/the-complete-list-of-changes-to-make-to-activate-client-certificate-mapping-on-iis-using-active-directory/.

For an environment without Active Directory and/or Microsoft Enterprise Certificate Authority, see http://www.iis.net/configreference/system.webserver/security/authentication/iisclientcertificatemappingauthentication.

To configure IIS authorization based on the user identity indicated by the client's certificate, see the section Configuring URL Authorization in https://docs.microsoft.com/en-us/iis/manage/configuring-security/understanding-iis-url-authorization.

10 Managing Logon Banner

{FTA_TAB.1:G:1}

10.1 Local Administrator Guidance

The following TechNet topics describe how to configure a message to users attempting to logon:

- Interactive logon: Message title for users attempting to log on: https://technet.microsoft.com/en-us/library/jj852182(v=ws.11).aspx
- Interactive logon: Message text for users attempting to log on: https://technet.microsoft.com/en-us/library/jj852199(v=ws.11).aspx

[i] The information in this link applies to the Windows 10 and Windows Server 2012 R2 as well as Windows Server 2016.