

## PP-Module for Client Virtualization Systems

This page is best viewed with JavaScript enabled!



Version: 1.1

2020-11-17

National Information Assurance Partnership

# Revision History

Version	Date	Comment
1.0	2016-11-17	Initial Publication
1.1	2020-11-17	Converted to <a href="#">PP-Module</a> and applied all active TDs

## Contents

[1Introduction](#)[1.1Overview](#)[1.2Terms](#)[1.2.1Common Criteria Terms](#)[1.2.2Technical Terms](#)[1.3Compliant Targets of Evaluation](#)[1.3.1TOE Boundary](#)[1.4Use Cases](#)[2Conformance Claims](#)[3Security Problem Description](#)[3.1Threats](#)[3.2Assumptions](#)[3.3Organizational Security Policies](#)[4Security Objectives](#)[4.1Security Objectives for the TOE](#)[4.2Security Objectives for the Operational Environment](#)[4.3Security Objectives Rationale](#)[5Security Requirements](#)[5.0.11Virtualization PP Security Functional Requirements Direction](#)[5.1.1 Modified SFRs](#)[5.2TOE Security Functional Requirements](#)[5.3Auditable Events for Mandatory SFRs](#)[5.03.21Security Management \(FMT\)](#)[5.4TOE Security Functional Requirements Rationale](#)[6Consistency Rationale](#)[6.1 Protection Profile for Virtualization](#)[6.1.1 Consistency of TOE Type](#)[6.1.2 Consistency of Security Problem Definition](#)[6.1.3 Consistency of Objectives](#)[6.1.4 Consistency of Requirements](#)[Appendix A - Entropy](#)[1.1 National Information Assurance Partnership 2020-11-17 Client Virtualization 1.0 2016-11-17 Initial Publication 1.1 2020-11-17 Converted to PP-Module and applied all active TDs](#)[Optional SFRs](#)[A.1Strictly Optional Requirements](#)[A.2Objective Requirements](#)[A.3Implementation-Dependent Requirements](#)[Appendix B - Selection-based SFRs](#)[Appendix C - Extended Component Definitions](#)[C.1Extended Components Table](#)[C.2Extended Component Definitions](#)[Appendix D - Entropy](#)[Appendix E - Bibliography](#)[Appendix F - Acronyms](#)

# 1 Introduction

## 1.1 Overview

The scope of this [PP-Module](#) is to define the security functionality of a Client Virtualization product in terms of [CC](#) and to define functional and assurance requirements for such products. This [PP-Module](#) is not complete in itself, but rather is intended for use with the following base [PP](#):

- Protection Profile for Virtualization, Version 1.1.

This base [PP](#) is valid because Client Virtualization is a specific type of Virtualization System and is expected to implement security functionality that is not common to all Virtualization Systems. One additional [SFR](#) has been defined in this [PP-Module](#) to define security functionality that is unique to this particular type of Virtualization System.

## 1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

### 1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a <a href="#">TOE</a> meets the SFRs <a href="#">[CC]</a> .
Base Protection Profile ( <a href="#">Base-PP</a> )	Protection Profile used as a basis to build a <a href="#">PP-Configuration</a> .
Common Criteria ( <a href="#">CC</a> )	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology ( <a href="#">CEM</a> )	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed <a href="#">TOE</a>	A <a href="#">TOE</a> composed of multiple components operating as a logical whole.
Operational Environment ( <a href="#">OE</a> )	Hardware and software that are outside the <a href="#">TOE</a> boundary that support the <a href="#">TOE</a> functionality and security policy.
Protection Profile ( <a href="#">PP</a> )	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration ( <a href="#">PP-Configuration</a> )	A comprehensive set of security requirements for a product type that consists of at least one <a href="#">Base-PP</a> and at least one <a href="#">PP-Module</a> .

Protection Profile Module ( <a href="#">PP-Module</a> )	An implementation-independent statement of security needs for a <a href="#">TOE</a> type complementary to one or more Base Protection Profiles.
Security Assurance Requirement ( <a href="#">SAR</a> )	A requirement to assure the security of the <a href="#">TOE</a> .
Security Functional Requirement ( <a href="#">SFR</a> )	A requirement for security enforcement by the <a href="#">TOE</a> .
Security Target ( <a href="#">ST</a> )	A set of implementation-dependent security requirements for a specific product.
<a href="#">TOE</a> Security Functionality ( <a href="#">TSF</a> )	The security functionality of the product under evaluation.
<a href="#">TOE</a> Summary Specification ( <a href="#">TSS</a> )	A description of how a <a href="#">TOE</a> satisfies the SFRs in an <a href="#">ST</a> .
Target of Evaluation ( <a href="#">TOE</a> )	The product under evaluation.

### 1.2.2 Technical Terms

Administrator	Administrators perform management activities on the <a href="#">VS</a> . These management functions do not include administration of software running within Guest VMs, such as the Guest <a href="#">OS</a> . Administrators need not be human as in the case of embedded or headless VMs. Administrators are often nothing more than software entities that operate within the <a href="#">VM</a> .
Domain	A Domain or Information Domain is a policy construct that groups together execution environments and networks by sensitivity of information and access control policy. For example, classification levels represent information domains. Within classification levels, there might be other domains representing communities of interest or coalitions. In the context of a <a href="#">VS</a> , information domains are generally implemented as collections of VMs connected by virtual networks. The <a href="#">VS</a> itself can be considered an Information Domain, as can its Management Subsystem.
Guest Operating System ( <a href="#">OS</a> )	An operating system that runs within a Guest <a href="#">VM</a> .
Guest <a href="#">VM</a>	A Guest <a href="#">VM</a> is a <a href="#">VM</a> that contains a virtual environment for the execution of an independent computing system. Virtual environments execute mission workloads and implement customer-specific client or server functionality in Guest VMs, such as a web server or desktop productivity applications.
Host Operating System ( <a href="#">OS</a> )	An operating system onto which a <a href="#">VS</a> is installed. Relative to the <a href="#">VS</a> , the Host <a href="#">OS</a> is part of the Platform.
Hypercall	An API function that allows <a href="#">VM</a> -aware software running within a <a href="#">VM</a> to invoke <a href="#">VMM</a> functionality.
Hypervisor	The Hypervisor is part of the <a href="#">VMM</a> . It is the software executive of the physical platform of a <a href="#">VS</a> . A Hypervisor's primary function is to mediate access to all CPU and memory resources, but it is also responsible for either the direct management or the delegation of the management of all other hardware devices on the hardware platform.
Management Subsystem	Components of the <a href="#">VS</a> that allow <a href="#">VS</a> Administrators to configure and manage the <a href="#">VMM</a> , as well as configure Guest VMs. <a href="#">VMM</a> management functions include <a href="#">VM</a> configuration, virtualized network configuration, and allocation of physical resources.
Platform	The hardware, firmware, and software environment into which a <a href="#">VS</a> is installed and executes.
User	Users operate Guest VMs and are subject to configuration policies applied to the <a href="#">VS</a> by Administrators. Users need not be human as in the case of embedded or headless VMs, users are often nothing more than software entities that operate within the <a href="#">VM</a> .
Virtual Machine ( <a href="#">VM</a> )	A Virtual Machine is a virtualized hardware environment in which an operating system may execute.
Virtual Machine Manager ( <a href="#">VMM</a> )	A <a href="#">VMM</a> is a collection of software components responsible for enabling VMs to function as expected by the software executing within them. Generally, the <a href="#">VMM</a> consists of a Hypervisor, Service VMs, and other components of the <a href="#">VS</a> , such as virtual devices, binary translation systems, and physical device drivers. It manages concurrent execution of all VMs and virtualizes platform resources as needed.
Virtualization System ( <a href="#">VS</a> )	A software product that enables multiple independent computing systems to execute on the same physical hardware platform without interference from one another. For the purposes of this document, the <a href="#">VS</a> consists of a Virtual Machine Manager ( <a href="#">VMM</a> ), Virtual Machine abstractions, a management subsystem, and other components.

## 1.3 Compliant Targets of Evaluation

Client Virtualization, for the purposes of this [PP-Module](#), refers to a Virtualization System that implements virtualized hardware components locally on an endpoint machine. Endpoints are typically client hardware such as desktop or laptop computers that a user interacts with directly, but may also include headless embedded systems without direct human interaction. A Virtualization System creates a virtualized hardware environment for each instance of a guest operating system (a virtual machine) permitting these environments to execute concurrently while maintaining isolation and the appearance of exclusive control over assigned computing resources. Client virtualization is generally used on endpoint systems, making use of the local machine's resources (memory, CPU, etc.) to provide isolated user environments.

This document does not address virtualization on mobile devices (typically devices that use a baseband processor or connect to a cellular network), nor does it address application virtualization or containers.

### 1.3.1 TOE Boundary

The [TOE](#) boundary is the same as that which is defined for a Virtualization System in general. Refer to the base Virtualization [PP](#) for an outline of the [TOE](#) boundary.

## 1.4 Use Cases

Requirements in this [PP-Module](#) are designed to address the security problem in the following use cases. The description of these use cases provides examples for how the [TOE](#) and its Operational Environment could support the functionality required by this [PP-Module](#).

#### [USE CASE 1] Locally Managed Client

A local administrator creates and runs one or more VMs locally. This client could be stand-alone or connected to a network.

#### [USE CASE 2] Enterprise Managed Client

An enterprise administrator for the [VS](#) centrally manages one or more client hypervisors, creating and configuring VMs which are then pushed to the clients. These VMs are then available for users on that client to run using the computing resources of that client. (Note that this is not Virtual Desktop Infrastructure where the hypervisors and the VMs run on remote servers. While both can be centrally managed and accessed from clients, for client virtualization, the VMs are local to the endpoint machine.)

#### [USE CASE 3] Headless Client

A [VM](#) is used by a program without direct human interaction.

## 2 Conformance Claims

### Conformance Statement

This [PP-Module](#) inherits exact conformance as required from the Virtualization [PP](#) and as defined in the [CC](#) and [CEM](#) addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

There are no other [PP](#)-Modules that are allowed to be specified in a [PP-Configuration](#) with this [PP-Module](#).

### CC Conformance Claims

This [PP](#) Module is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Release 5 [\[CC\]](#).

## 3 Security Problem Description

The security problem is described in terms of the threats that the [TOE](#) is expected to address, assumptions about its operational environment, and any organizational security policies that the [TOE](#) is expected to enforce.

### 3.1 Threats

This [PP-Module](#) defines no additional threats beyond those defined in the base Virtualization [PP](#). Note however that the SFRs defined in this [PP-Module](#) will assist in the mitigation of the following threats defined in the base [PP](#):

#### T.UNAUTHORIZED\_UPDATE

See Virtualization [PP](#), Section 3.1.

#### T.UNAUTHORIZED\_ACCESS

See Virtualization [PP](#), Section 3.1.

### 3.2 Assumptions

This [PP-Module](#) does not define any assumptions.

### 3.3 Organizational Security Policies

This [PP-Module](#) defines no additional Organizational Security Policies.

## 4 Security Objectives

### 4.1 Security Objectives for the TOE

This [PP-Module](#) defines no additional [TOE](#) security objectives beyond those defined in the base Virtualization [PP](#). Note however that the [SFR](#) defined in this [PP-Module](#) will assist in the achievement of the following objectives defined in the base [PP](#):

- O.VMM\_INTEGRITY  
See Virtualization [PP](#), Section 4.1.
- O.MANAGEMENT\_ACCESS  
See Virtualization [PP](#), Section 4.1.

### 4.2 Security Objectives for the Operational Environment

This [PP-Module](#) does not define any objectives for the Operational Environment. Because this Module does not define any additional assumptions or organizational security policies, there are no additional security objectives for the Operational Environment to satisfy.

### 4.3 Security Objectives Rationale

This section describes how the assumptions, threats, and organization security policies map to the security objectives.

Table 1: Security Objectives Rationale

Threat, Assumption, or OSP	Security Objectives	Rationale
<a href="#">T.UNAUTHORIZED_UPDATE</a>	<a href="#">O.VMM_INTEGRITY</a>	Integrity of a Virtualization System can be maintained by ensuring that the only way to modify the <a href="#">VS</a> is through a trusted update process initiated by an authorized Administrator as required by <a href="#">FMT_MOF_EXT</a> .
<a href="#">T.UNAUTHORIZED_ACCESS</a>	<a href="#">O.MANAGEMENT_ACCESS</a>	Access to management functions must be limited to authorized Administrators as managed through controls required by <a href="#">FMT_MOF_EXT.1</a> .

## 5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [\[CC\]](#). The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): is used to add details to a requirement (including replacing an assignment with a more restrictive selection) or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): is used to select one or more options provided by the [\[CC\]](#) in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: is indicated by appending the [SFR](#) name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

### 5.1 Virtualization PP Security Functional Requirements Direction

In a [PP-Configuration](#) that includes the Virtualization [PP](#), the [TOE](#) is expected to rely on some of the security functions implemented by the Virtualization System as a whole and evaluated against the [Base-PP](#). This section describes any modifications that the [ST](#) author must make to [Base-PP](#) SFRs to satisfy the required [VS](#) functionality. ~~When this~~

#### 5.1.1 Modified SFRs

~~This [PP-Module](#) is used to extend does not modify any SFRs defined by the Virtualization [PP](#), the [TOE](#) type for the overall [TOE](#) is still a Virtualization System. The [TOE](#) boundary does not change. This threat applies to functionality that is described in the base [PP](#), but is managed through functionality described in this [PP](#) module. This threat applies to functionality that is described in the base [PP](#), but is managed through functionality described in this [PP](#) module. 5.0.1.~~

## 5.2 TOE Security Functional Requirements

The following section describes the SFRs that must be satisfied by any [TOE](#) that claims conformance to this [PP-Module](#). These SFRs must be claimed regardless of which [PP-Configuration](#) is used to define the [TOE](#).

## 5.3 Auditable Events for Mandatory SFRs

Table

**Table 2: Auditable Events for Mandatory SFRs**

Requirement	Auditable Events	Additional Audit Record Contents
<a href="#">FMT_MOF_EXT.1</a>	No events specified	

### 5.03.2-1 Security Management (FMT)

This family is defined in the Virtualization [PP](#). This Module augments the extended family by adding one additional component,

#### [FMT\\_MOF\\_EXT.1](#)

#### [FMT\\_MOF\\_EXT.1](#) Management of Security Functions Behavior

This [SFR](#) requires the Server Virtualization product to manage security functionality defined in the Virtualization [PP](#) in [FPT\\_TUD\\_EXT.1](#), [FIA\\_PMG\\_EXT.1](#), [FDP\\_VNC\\_EXT.1](#), [FDP\\_VMS\\_EXT.1](#), [FMT\\_MSA\\_EXT.1](#), [FPT\\_HCL\\_EXT.1](#), [FPT\\_RDM\\_EXT.1](#), [FIA\\_AFL\\_EXT.1](#), and [FTA\\_TAB.1](#).

defines required management functions and responsibilities. There are no additional management functions beyond those already described in [FMT\\_MOF\\_EXT.1](#).

There are no auditable events defined for this [SFR](#). No other dependencies.

#### [FMT\\_MOF\\_EXT.1.1](#)

The [TSF](#) shall be capable of supporting [selection: *local*, *remote*] administration.

Application Note: Selection of “remote” requires the selection-based requirement [FPT\\_TRP.1](#) defined in the base [PP](#) to be included in the [ST](#).

#### [FMT\\_MOF\\_EXT.1.2](#)

The [TSF](#) shall be capable of performing the following management functions, controlled by an Administrator or User as shown in [Table 2.3](#), based on the following key:

**Table 2.3: Client Virtualization Management Functions**

X = Mandatory ( <a href="#">TOE</a> must provide that function to that role)				
O = Optional ( <a href="#">TOE</a> may or may not provide that function to that role)				
N = Not Permitted ( <a href="#">TOE</a> must not provide that function to that role)				
S = Selection-Based ( <a href="#">TOE</a> must provide that function to that role if the <a href="#">TOE</a> claims a particular selection-based <a href="#">SFR</a> )				
Number	Function	Administrator	User	Notes (all <a href="#">SFR</a> references are from the base Virtualization <a href="#">PP</a> )
1	Ability to update the Virtualization System	X	N	See <a href="#">FPT_TUD_EXT.1</a>
2	[selection: <i>Ability to configure Administrator password policy as defined in <a href="#">FIA_PMG_EXT.1</a>. Not applicable.</i> ]	S	N	Must be selected if <a href="#">ST</a> includes <a href="#">FIA_PMG_EXT.1</a> .
3	Ability to create, configure and delete VMs	X	O	
4	Ability to set default initial <a href="#">VM</a> configurations	X	O	
5	Ability to configure virtual networks including <a href="#">VM</a>	X	O	See <a href="#">FDP_VNC_EXT.1</a>
6	Ability to configure and manage the audit system and audit data	X	N	
7	Ability to configure <a href="#">VM</a> access to physical devices	X	O	See <a href="#">FDP_PPR_EXT.1</a>
8	Ability to configure inter-VM data sharing	X	O	See <a href="#">FDP_VMS_EXT.1</a> and <a href="#">FMT_MSA_EXT.1</a>
9	Ability to enable/disable <a href="#">VM</a> access to Hypercall functions	X	O	See <a href="#">FPT_HCL_EXT.1</a>
10	Ability to configure removable media policy	X	O	See <a href="#">FPT_RDM_EXT.1</a>
11	Ability to configure the cryptographic functionality	O	O	See <a href="#">FCS_CKM.1</a> , <a href="#">FCS_CKM.2</a> , and



12	Ability to change default authorization factors	X	N	ECS_COP.1/HASH See FIA_PMG_EXT.1
13	Ability to enable/disable screen lock	O	O	
14	Ability to configure screen lock inactivity timeout	O	O	
15	Ability to configure remote connection inactivity timeout	X	N	
16	Ability to configure lockout policy for unsuccessful authentication attempts through [selection: <u>timeouts between attempts, limiting number of attempts during a time period</u> ]	X	N	See FIA_AFL_EXT.1
17	[selection: <u>Ability to configure name/address of directory server to bind with, Not applicable</u> ]	S	O	Must be selected if "directory-based" is selected anywhere in FIA_UAU.5.1 in the base Virtualization PP.
18	Ability to configure name/address of audit/logging server to which to send audit/logging records	X	N	See FAU_STG_EXT.1. Must be selected if "directory-based" is selected anywhere in FIA_UAU.5.1 in the base Virtualization PP.
19	Ability to configure name/address of network time server	X	O	
20	Ability to configure banner	X	N	See FTA_TAB.1
21	Ability to connect/disconnect removable devices to/from a VM	O	O	See FPT_RDM_EXT.1
22	Ability to start a VM	O	O	
23	Ability to stop/halt a VM	O	O	
24	Ability to checkpoint a VM	O	O	
25	Ability to suspend a VM	O	O	
26	Ability to resume a VM	O	O	
27	[selection: <u>Ability to configure action taken if unable to determine the validity of a certificate, Not applicable</u> ]	S	N	This function must be selected if "allow the administrator to choose whether to accept the certificate in these cases" in FIA_X509_EXT.2.2 in the base PP.

The TSF shall be capable of performing the following management functions assignment: description of management functions.

Application Note: The ST author is expected to update Table 2.3 with an indication as to whether any of the 'optional' or 'selection-based' functions are included as part of the TOE. The ST author may also omit the 'Notes' column as it is provided in this PP-Module as an aid to the ST author in constructing the table.

This SFR addresses the roles of the CC Part 2 SFRs FMT\_MOF.1, FMT\_SMF.1, and FMT\_SMR.2.

Administration is considered "local" if the Administrator is physically present at the machine on which the VS is installed.

Administration is considered "remote" if communications between the Administrator and the Management Subsystem travel on a network.

There is no requirement to authenticate Users of the Virtualization System. Users that have access to VMs but not to the Management Subsystem need not authenticate to the Virtualization System in order to use Guest VMs. Requirements for authentication of VM users is determined by the policies of the domains running within the Guest VMs.

For a VS where the OS is part of the platform and not part of the TOE, it is acceptable for the VS to invoke the Host OS screen lock.

#### Evaluation Activity

##### TSS

The evaluator shall examine the TSS and Operational Guidance to ensure that it describes which security management functions require Administrator privilege and the actions associated with each management function. The evaluator shall verify that for each management function and role specified in Table 2, the defined role is able to perform all mandatory functions as well as all optional or selection-based functions claimed in the ST.

#### Guidance

The evaluator shall examine the Operational Guidance to ensure that it describes how the Administrator and/or User are able to perform each management function that the ST claims the TOE supports.

The evaluator shall verify for each claimed management function that the Operational Guidance is sufficiently detailed to allow the function to be performed and that the function can be performed.

#### Tests

The evaluator shall test each management function for each role listed in the FMT\_MOF\_EXT.1.1 table Table 2 in the ST to demonstrate that the function can be performed by the role(s) that are authorized to do so and the result of the function is demonstrated. The evaluator shall also verify for each claimed management function in Table 2 that if the TOE claims not to

provide a particular role with access to the function, then it is not possible to access the [TOE](#) as that role and perform that function.

Appendix A

5.4 TOE Security Functional Requirements Rationale

The following rationale provides justification for each security objective for the [TOE](#), showing that the SFRs are suitable to meet and achieve the security objectives:

Table 4: <a href="#">SFR Rationale</a>		
OBJECTIVE	ADDRESSED BY	RATIONALE
<a href="#">O.VMM_INTEGRITY</a>	<a href="#">FMT_MOF_EXT.1</a>	Integrity of a Virtualization System can be maintained by ensuring that the only way to modify the <a href="#">VS</a> is through a trusted update process initiated by an authorized Administrator as required by <a href="#">FMT_MOF_EXT.1</a> .
<a href="#">O.MANAGEMENT_ACCESS</a>	<a href="#">FMT_MOF_EXT.1</a>	Access to management functions must be limited to authorized Administrators as managed through controls required by <a href="#">FMT_MOF_EXT.1</a> .

6 Consistency Rationale

6.1 Protection Profile for Virtualization

6.1.1 Consistency of TOE Type

When this [PP-Module](#) is used to extend the Virtualization [PP](#), the [TOE](#) type for the overall [TOE](#) is still a Virtualization System. The [TOE](#) boundary does not change.

6.1.2 Consistency of Security Problem Definition

The threats, assumptions, and OSPs defined by this [PP-Module](#) (see section 3.1) supplement those defined in the Virtualization [PP](#) as follows:

<a href="#">PP-Module</a> Threat, Assumption, OSP	Consistency Rationale
<a href="#">T.UNAUTHORIZED_UPDATE</a>	This threat comes directly from the <a href="#">PP</a> .
<a href="#">T.UNAUTHORIZED_ACCESS</a>	This threat comes directly from the <a href="#">PP</a> .

6.1.3 Consistency of Objectives

The objectives for the TOEs are consistent with the Virtualization [PP](#) based on the following rationale:

<a href="#">PP-Module</a> <a href="#">TOE</a> Objective	Consistency Rationale
<a href="#">O.VMM_INTEGRITY</a>	This objective comes directly from the <a href="#">PP</a> .
<a href="#">O.MANAGEMENT_ACCESS</a>	This objective comes directly from the <a href="#">PP</a> .

6.1.4 Consistency of Requirements

This [PP-Module](#) identifies several SFRs from the Virtualization [PP](#) that are needed to support Client Virtualization Systems functionality. This is considered to be consistent because the functionality provided by the Virtualization [PP](#) is being used for its intended purpose. The rationale for why this does not conflict with the claims defined by the Virtualization [PP](#) are as follows:

<a href="#">PP-Module</a> Requirement	Consistency Rationale
	<b>Modified SFRs</b>
	This <a href="#">PP-Module</a> does not modify any requirements when the Virtualization <a href="#">PP</a> is the base.
	<b>Mandatory SFRs</b>
<a href="#">FMT_MOF_EXT.1</a>	This <a href="#">SFR</a> requires the Client Virtualization product to manage security functionality defined in the Virtualization <a href="#">PP</a> in <a href="#">FPT_TUD_EXT.1</a> , <a href="#">FIA_PMG_EXT.1</a> , <a href="#">FDP_VNC_EXT.1</a> , <a href="#">FDP_PPR_EXT.1</a> , <a href="#">FDP_VMS_EXT.1</a> , <a href="#">FMT_MSA_EXT.1</a> , <a href="#">FPT_HCL_EXT.1</a> , <a href="#">FPT_RDM_EXT.1</a> , <a href="#">FCS_CKM.1</a> , <a href="#">FCS_CKM.2</a> , <a href="#">FCS_COP.1/HASH</a> , <a href="#">FIA_AFL_EXT.1</a> , <a href="#">FAU_STG_EXT.1</a> , <a href="#">FIA_X509_EXT.2.2</a> , and <a href="#">FTA_TAB.1</a> .



### Optional SFRs

This [PP-Module](#) does not define any Optional requirements.

### Selection-based SFRs

This [PP-Module](#) does not define any Selection-based requirements.

### Objective SFRs

This [PP-Module](#) does not define any Objective requirements.

### Implementation-Dependent SFRs

This [PP-Module](#) does not define any Implementation-Dependent requirements.

## Appendix A - Optional SFRs

### A.1 Strictly Optional Requirements

This [PP-Module](#) does not define any Optional SFRs.

### A.2 Objective Requirements

This [PP-Module](#) does not define any Objective SFRs.

### A.3 Implementation-Dependent Requirements

This [PP-Module](#) does not define any Implementation-Dependent SFRs.

## Appendix B - Selection-based SFRs

This [PP-Module](#) does not define any selection-based SFRs.

## Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the [PP-Module](#).

### C.1 Extended Components Table

All extended components specified in the [PP](#) are listed in this table:

**Table 5: Extended Component Definitions**

Functional Class	Functional Components
Security Management (FMT)	FMT_MOF_EXT Management of Security Functions Behavior

### C.2 Extended Component Definitions

#### FMT\_MOF\_EXT Management of Security Functions Behavior

This family is defined in the Virtualization [PP](#). This Module augments the extended family by adding one additional component, [FMT\\_MOF\\_EXT.1](#).

#### Component Leveling

[FMT\\_MOF\\_EXT.1](#), Management of Security Functions Behavior, defines required management functions and responsibilities.

#### Management: FMT\_MOF\_EXT.1

There are no additional management functions beyond those already described in [FMT\\_MOF\\_EXT.1](#).

#### Audit: FMT\_MOF\_EXT.1

There are no auditable events defined for this [SFR](#).

#### FMT\_MOF\_EXT.1 Management of Security Functions Behavior

Hierarchical to: No other components.

Dependencies to: No other dependencies.

### FMT\_MOF\_EXT.1.1

The [TSF](#) shall be capable of supporting **[selection: *local, remote*]** administration.

### FMT\_MOF\_EXT.1.2

The [TSF](#) shall be capable of performing the following management functions **assignment**: description of management functions].

## Appendix D - Entropy

The [TOE](#) does not require any additional supplementary information to describe its entropy source(s) beyond the requirements outlined in the 'Entropy Documentation and Assessment' section of the Base Virtualization [PP](#). As with other base [PP](#) requirements, the only additional requirement is that the entropy documentation also applies to the specific Client Virtualization capabilities of the [TOE](#) in addition to the functionality required by the base [PP](#).

## Appendix E - Bibliography

### Identifier

### Title

Common Criteria for Information Technology Security Evaluation -

[CC]

- [Part 1: Introduction and General Model](#), CCMB-2017-04-001, Version 3.1, Revision 5, April 2017.
- [Part 2: Security Functional Components](#), CCMB-2017-04-002, Version 3.1, Revision 5, April 2017.
- [Part 3: Security Assurance Components](#), CCMB-2017-04-003, Version 3.1, Revision 5, April 2017.

[VirtPP] Protection Profile for Virtualization, Version: 1.1, 2020-11-17

## Appendix F - Acronyms

Acronym	Meaning
<a href="#">Base-PP</a>	Base Protection Profile
<a href="#">CC</a>	Common Criteria
<a href="#">CEM</a>	Common Evaluation Methodology
<a href="#">OE</a>	Operational Environment
<a href="#">OS</a>	Operating System
<a href="#">PP</a>	Protection Profile
<a href="#">PP-Configuration</a>	Protection Profile Configuration
<a href="#">PP-Module</a>	Protection Profile Module
<a href="#">SAR</a>	Security Assurance Requirement
<a href="#">SFR</a>	Security Functional Requirement
<a href="#">ST</a>	Security Target
<a href="#">TOE</a>	Target of Evaluation
<a href="#">TSF</a>	<a href="#">TOE</a> Security Functionality
<a href="#">TSFI</a>	<a href="#">TSF</a> Interface
<a href="#">TSS</a>	<a href="#">TOE</a> Summary Specification
<a href="#">VM</a>	Virtual Machine
<a href="#">VMM</a>	Virtual Machine Manager
<a href="#">VS</a>	Virtualization System