PP-Module for Host Agent

Version: 1.0

2020-01-31

National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2020-01-31	Draft - first version released

Contents

1 Introduction

1.1 Overview

The scope of this PP-Module is to describe the security functionality of a Host Agent in terms of CC and to define functional and assurance requirements for such products. This Module is not complete in itself, but rather uses the Protection Profile for Application Software [AppPP] as a Base-PP. The combined requirements in this Host Agent Module with the Application Software PP is meant to be paired with an evaluation using an Enterprise Security Management (ESM) Protection Profile. The ESM PP covers the security functionality needed on the server or cloud service, and the paired Host Agent Module covers the security functionality needed on the endpoint device (desktop, mobile device, etc.). At this time only the ESM [EDR] PP is published and ready for use with this Host Agent Module. Future versions of this Module will include requirements for other classes of Enterprise Security Management software.

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 TOE meets the SFRs [CC].
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in a ST.
Target of Evaluation (TOE)	The product under evaluation.

1.2.2 Technical Terms

Endpoint	A computing device that runs a general purpose OS, mobile device OS, or network device OS. Endpoints can include desktops, servers, and mobile devices.
Endpoint Detection and Response (EDR)	A system that analyzes collected EDR Host Agent data for detecting, investigating, and remediating unauthorized activities on endpoints.
Enrolled State	The state in which an endpoint with a running Host Agent is managed by an ESM. Also, referred to as Onboarding.
Enrollment	The process of transitioning an endpoint from an unenrolled to an enrolled state.
Enterprise Security Management	A enterprise security management application hosted on a server or cloud service that provides support for security management, information flows, reporting, policy, and data analytics in complex enterprise environments.

(ESM)	
Host Agent	A logical piece of software that executes on endpoints to collect data about the endpoint and executes commands sent to the endpoint from an Enterprise Security Management (ESM) server or service. An example command sent to an endpoint could be to enforce a policy from an ESM, to collect some files, or to run an OS command.
Operating System (OS)	Software that manages physical and logical resources and provides services for applications.
Unenrolled State	The state in which an endpoint, with or without a Host Agent, is not managed by an ESM. Also, referred to as Offboarding.

1.3 Compliant Targets of Evaluation

1.3.1 TOE Boundary

The boundary for the Host Agent includes all processes, all modules and libraries bundled with the Host Agent. The Host Agent can run as a daemon or service on the platform but is not required to. The Host Agent is not expected to have a local or remote Graphical User Interface (GUI) for administration but having such an interface is not precluded by this Module. It is expected that Host Agents will be managed by their associated ESM Server or the underlying platform. The TOE boundary includes the communications channel with other Host Agents, an ESM Server, or a cloud service. The platform operating system or execution environment upon which the Host Agent is executing is outside the scope of a Host Agent evaluation. The figures below show some sample Host Agents but are not inclusive of every possible Host Agent design.

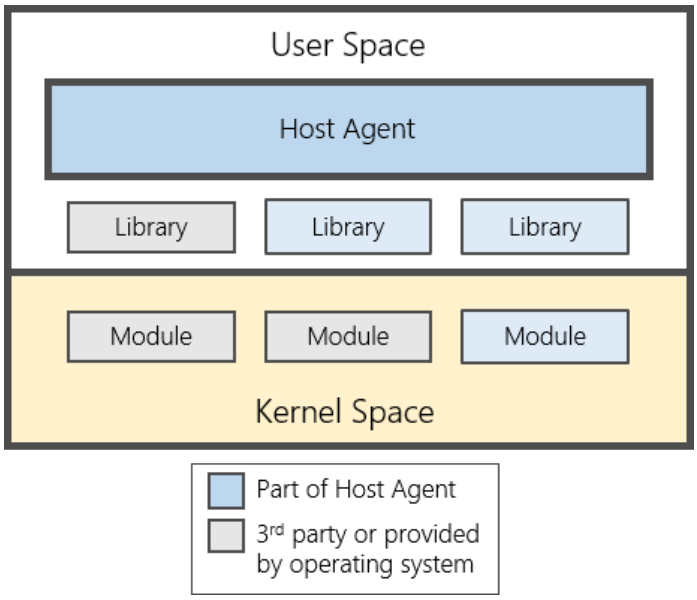

Figure 1: Sample Host Agent TOE

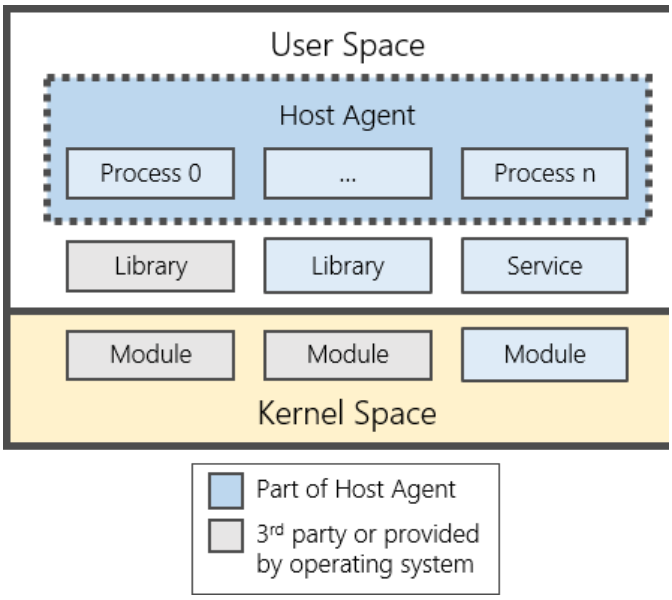

Figure 2: Sample Host Agent TOE

1.3.2 TOE Platform

The TOE platform consists of a general purpose OS, a mobile device OS, a network device OS, or an Execution Environment on top of which the Host Agent software executes.

1.4 Use Cases

Requirements in this Protection Profile are designed to address the security problems in at least the following use cases. These use cases are intentionally very broad, as many specific use cases exist for an operating system. These use cases may also overlap with one another. An operating system's functionality may even be effectively extended by privileged applications installed onto it. However, these are out of scope of this PP.

[USE CASE 1] Communication

The Host Agent allows for communication interactively or non-interactively with other Enterprise Security Management (ESM) software over a communications channel. Example communications include but are not limited to; receiving policy, sending data and running tasks or commands.

2 Conformance Claims

Conformance Statement

This inherits exact conformance as required from the specified and as defined in the and addenda for Exact Conformance, Selection-Based SFRs, and Optional SFRs (dated May 2017).

CC Conformance Claims

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

Package Claims

This is TLS Package Version 1.1 Conformant.

3 Security Problem Description

The security problem is described in terms of the threats that the Host Agent is expected to address, assumptions about the operational environment, and any organizational security policies that the Host Agent is expected to enforce.

3.1 Threats

Note that this PP-Module does not repeat the threats identified in the [AppPP], though they all apply given the conformance and hence dependence of this PP-Module on the [AppPP].

T.DATA_LOSS
A Host Agent can be susceptible to data loss during periods when connectivity to the Enterprise Security Management (ESM) system is not present.

T.TAMPER
A Host Agent can be susceptible to tampering by unprivileged users who may try to uninstall or disrupt the Host Agent's ability to function properly.

3.2 Assumptions

These assumptions are made on the Operational Environment in order to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an Operational Environment that does not meet these assumptions, the TOE may no longer be able to provide all of its security functionality.

3.3 Organizational Security Policies

This PP-Module defines no additional organizational security policies beyond those defined in the Base-PP.

4 Security Objectives

4.1 Security Objectives for the TOE

O.ACCOUNTABILITY

Conformant Host Agents ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the Host Agent.

Addressed by: FAU_GEN.1, FAU_STO_EXT.1

O.DATA_RECORDER

Conformant Host Agents ensure that specific security information is cached or queued during periods when the trusted channel is not available. This will prevent data loss of Host Agent data and allow for proper remediation.

Addressed by: FHA_CHA_EXT.1 (selection-based), FHA_COL_EXT.1 (selection-based), FHA_HAD_EXT.1

O.INTEGRITY

Conformant Host Agents will ensure the integrity of policy and/or commands sent to the Host Agent and also leverage execution environment or platform-based mitigations to protect the Host Agent.

Addressed by: FMT_POL_EXT.1 (objective), FMT_UNR_EXT.1

O.MANAGEMENT

To facilitate management by the enterprise, conformant Host Agents provide consistent and supported interfaces for their security-relevant configuration and maintenance.

Addressed by: FMT_SMF.1/1

O.PROTECTED_COMMS

To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant Host Agents will use a trusted channel for sending and receiving data.

Addressed by: FTP_DIT_EXT.1 (from Base-PP), FTP_DIT_EXT.2 (selection-based)

4.2 Security Objectives for the Operational Environment

This module does not define any objectives for the Operational Environment. The following security objectives for the operational environment assist the Host Agent in correctly providing its security functionality. These track with the assumptions about the environment.

4.3 Security Objectives Rationale

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

Threat, Assumption, or OSP	Security Objectives	Rationale
T.DATA_LOSS	O.DATA_RECORDER	The threat T.DATA_LOSS is countered by O.DATA_RECORDER as this provides for caching of data by a Host Agent during periods when not connected to the ESM system.
T.TAMPER	O.ACCOUNTABILITY, O.INTEGRITY	The threat T.TAMPER is countered by O.ACCOUNTABILITY which protect the Host Agent and report artifact up to the ESM system that could help to discover tampering. The threat T.TAMPER is countered by O.INTEGRITY which protect the Host Agent and report artifact up to the ESM system that could help to discover tampering.

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 notations are used:

- **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 App PP Security Functional Requirements Direction

In a PP-Configuration that includes App PP, the TOE is expected to rely on some of the security functions implemented by the application as a whole and evaluated against the Base-PP. The SFRs listed in this section are defined in the Base-PP and relevant to the secure operation of the Host Agent. This section describes any modifications that the ST author must make to the Base-PP SFRs to satisfy the required Host Agent functionality.

5.1.1 Modified SFRs

The SFRs listed in this section are defined in the App Protection Profile and relevant to the secure operation of the TOE.

5.1.1.1 User Data Protection

FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1 The Host Agent shall restrict network communications to: [**selection**:

- *an ESM Server*,
- *another Host Agent*

]

Application Note: By selecting another Host Agent the additional FTP_DIT_EXT.2 requirements must be included in the ST for peer-to-peer communication.
This restricts the selections in the Base-PP to a specific list of communications that may be user or application initiated.

Evaluation Activity

TSS
The TSS is unchanged from the Base-PP.
Guidance
The guidance is unchanged from the Base-PP.
Tests
The tests are unchanged from the Base-PP.

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.

5.2.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation (Refined)

FAU_GEN.1.1 The Host Agent shall generate an audit record of the following auditable events:

a. Enrollment with an Enterprise Management System (Success/Failure);
b. Change in enrollment state with an Enterprise Management System;
c. [**selection**: *Receiving*, *Generating*] periodic heartbeat events
d. [**assignment**: *other specifically defined auditable events*]

.

Application Note: The required audit events must be generated by the Host Agent, but can leverage API's available from the platform if needed to generate the audit events. For the selection one or both options may be selected. The assignment may be empty, a single item, or multiple items.

FAU_GEN.1.2 The [**selection**: *Host Agent*, *Host Agent Platform*] shall record within each audit record at least the following information:

a. Date and time of the event,
b. Type of event,
c. Subject identity,
d. (Success or failure) of the event, if relevant,
e. [**assignment**: *Other audit relevant information*]

.

Application Note: All audits must contain at least the information mentioned in FAU_GEN.1.2, but may contain more information. The term *subject* here is understood to be the user that the process is acting on behalf of or for network communication related events the server name/address. The subject identity can be blank if not applicable for a given process. The assignment may be empty, a single item, or multiple items.

Evaluation Activity

TSS
The evaluator shall verify the TSS lists all record types that are recorded.

The evaluator shall verify that the TSS lists all the auditable event types and all audit information that the TOE records.
Guidance
The evaluator shall check the administrative guide and ensure that it lists all of the auditable events. The evaluator shall check to make sure that every audit event type selected in the ST is included.

The evaluator shall check the administrative guide and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator shall ensure that the fields contains the information required.
Tests
- ***Test 1:*** *The evaluator shall test the Host Agent's ability to correctly generate audit records by having the Host Agent generate audit records for each type of event listed in the ST.*
- ***Test 2:*** *The evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record provide the required information.*

FAU_STO_EXT.1 Audit Data Storage

FAU_STO_EXT.1.1 The [**selection**: *Host Agent*, *Host Agent Platform*] shall store audit events in the platform provided logging mechanism.

Application Note: The term *audit events* here is understood to be only the set of events defined in FAU_GEN.1. If the job of this Host Agent is to generate or collect events for an enterprise security management server it is not expected that those events will be stored in the platform provided logging mechanism.

Evaluation Activity

TSS
The evaluator shall verify the TSS contains details of where all audit data is stored.
Guidance
The evaluator shall check the administrative guide and ensure that the list of auditable events are stored in the platform provided logging mechanism.
Tests
- ***Test 1:*** *The evaluator shall test the Host Agent's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the ST. This should include all instance types of an event specified. When verifying the test results, the evaluator shall ensure the audit records generated during testing are stored in the platform provided logging mechanism.*
  On Linux based platforms this would be in var/logs. On Windows based platforms this would be the Windows Event Log.
  No specific locations are defined for other platforms.

5.2.2 Host Agent (FHA)

FHA_HAD_EXT.1 Host Agent Declaration

FHA_HAD_EXT.1.1 The Host Agent shall operate with the following ESM Software:

Endpoint Detection and Response (EDR)

Application Note: Currently, a NIAP PP only exists for EDR; Systems Management and Audit Server will be added later. By including EDR the additional FHA_CHA_EXT.1 and FHA_COL_EXT.1 requirements shall be included in the ST.

Evaluation Activity

TSS
The evaluator shall verify the TSS lists all classes of products the Host Agent is designed to function with.
Guidance
The evaluator shall check the administrative guide and ensure that guidence exists for enrollment with all compatible ESM products identified in the ST.
Tests

- ***Test 1:*** *Conditional: If EDR is selected the evaluator shall install the Host Agent and enroll it with the EDR management system. The evaluator shall verify that enrollment was successful and that the Host Agent is communicating with the EDR.*

5.2.3 Security Management (FMT)

FMT_SMF.1/1 Specification of Management Functions (Configuration of Host Agent)

FMT_SMF.1.1/1 The **Host Agent** shall be capable of the following management functions:

Management Function	Administrator
Configure the frequency for sending Host Agent data to an ESM	O
Assign at least one label or tag to categorize individual endpoint systems	O

Application Note: This requirement captures all the configuration functionality the TSF provides the administrator to configure the Host Agent. The configuration of these management functions can be achieved by either local configuration of the Host Agent or by remote configuration using the ESM Server. The frequency for sending data to an ESM can be specified as a time value, but does not have to be. A value like Aggressive, Normal, Low Bandwidth is a measure of control of frequency and meets the requirement. Host Agent data refers to the data collected in the requirements in this PP-Module, such as FHA_COL_EXT.1.1.

Evaluation Activity

TSS
The evaluator shall verify the TSS contains all frequencies for sending Host Agent data to an ESM and all labels that are permitted.
Guidance
The evaluator shall verify that every management function mandated by the PP-Module is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.
Tests

- ***Test 1:*** *The evaluator shall test the ability to configure the Host Agent and test each option from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.*

FMT_UNR_EXT.1 User Unenrollment Prevention

FMT_UNR_EXT.1.1 The [**selection**: *Host Agent*, *Host Agent Platform*] shall enforce a mechanism to prevent unprivileged users of the platform from unenrolling the Host Agent with the ESM system.

Application Note: Unenrolling is the action of transitioning from the enrolled state to the unenrolled state. Preventing unprivileged users from unenrolling the Host Agent provides assurance that the enterprise can manage connected endpoints.

Evaluation Activity

TSS
The evaluator shall ensure that the TSS describes the mechanism used to prevent users from unenrolling the Host Agent.
Guidance

There is no associated guidance for this requirement.

Tests

- ***Test 1:*** *The evaluator shall attempt to unenroll the Host Agent from the ESM system as an unprivileged user and verify that the attempt fails, by trying to kill the process or stop the Service or Daemon that is running the Host Agent.*

6 Consistency Rationale

6.1 Application Software Protection Profile

6.1.1 Consistency of TOE Type

If this PP-Module is used to extend the Application SoftwarePP, the TOE type for the overall TOE is still a software-based application. The TOE boundary is simply extended to include the Host Agent functionality that is built into the application so that additional security functionality is claimed within the scope of the TOE.

6.1.2 Consistency of Security Problem Definition

The threats defined by this PP-Module (see section 3.1) supplement those defined in the App PP as follows:

PP-Module Threat	Consistency Rationale
T.DATA_LOSS	This threat relates to the loss of data that is collected by theESM Host Agent. This relates to functionality defined by the PP-Module and does not interfere with the functionality described by the Base-PP.
T.TAMPER	This threat is an extension of the T.LOCAL_ATTACK threat defined by the Base-PP. The threat of tampering as applied to the PP-Module exists in addition to the local attacks that are possible on the capabilities defined by the Base-PP.

6.1.3 Consistency of Objectives

The objectives for the TOEs are consistent with the App PP based on the following rationale:

PP-Module TOE Objective	Consistency Rationale
O.ACCOUNTABILITY	This objective relates to the TOE's generation and storage of audit data that is used to detect potential configuration or operational issues on host systems. This functionality is defined by the PP-Module and does not affect the ability of the TOE to enforce the Base-PP's security objectives.
O.DATA_RECORDER	This objective relates to the availability of data collected by the TSF. This data is specified to ESM Host Agent functionailty and does not affect the functionality defined by the Base-PP.
O.INTEGRITY	This objective is the same as the Base-PP objective of the same name. This PP-Module extends the objective by defining additional requirements to satisfy the objective that relate to the specific functionality described by the PP-Module.
O.MANAGEMENT	This objective is the same as the Base-PP objective of the same name. This PP-Module extends the objective by defining additional requirements to satisfy the objective that relate to the specific functionality described by the PP-Module.
O.PROTECTED_COMMS	This objective is the same as the Base-PP objective of the same name. This PP-Module extends the objective by defining additional requirements to satisfy the objective that relate to the specific functionality described by the PP-Module.

This PP-Module does not define any objectives for theTOE's operational environment.

6.1.4 Consistency of Requirements

This PP-Module identifies several SFRs from the App PP that are needed to support Host Agent functionality. This is considered to be consistent because the functionality provided by the App is being used for its intended purpose. The PP-Module also identifies a number of modified SFRs from the App PP as well as new SFRs that are used entirely to provide functionality for Host Agent. The rationale for why this does not conflict with the claims defined by the App PP are as follows:

PP-Module Requirement	Consistency Rationale
	Modified SFRs
FDP_NET_EXT.1	
	Mandatory SFRs
FAU_GEN.1	The Base-PP does not define an audit mechanism for its own functionality. This function does not interfere with the Base-PP.
FAU_STO_EXT.1	The Base-PP does not define an audit mechanism for its own functionality. This function does not interfere with the Base-PP.
FHA_HAD_EXT.1	This SFR defines the type of software the Host Agent is intended to operate and communicate with. This relates to functionality not present in the Base-PP and does not affect the TOE's ability to satisfy the Base-PP's SFRs.

FMT_SMF.1/1	This SFR defines management functions for the SFRs defined in thisPP-Module. It does not affect the management functions defined in the Base-PP.
FMT_UNR_EXT.1	This SFR defines protections to prevent users from tampering with the Host Agent. This relates to functionality not present in the Base-PP and does not affect the TOE's ability to satisfy the Base-PP's SFRs.
Optional SFRs	
This PP-Module does not define any optional requirements.	
Selection-based SFRs	
FHA_CHA_EXT.1	This SFR defines how the Host Agent shall cache data locally. This relates to functionality not present in the Base-PP and does not affect the TOE's ability to satisfy the Base-PP's SFRs.
FHA_COL_EXT.1	This SFR defines the type of software the Host Agent is intended to operate with. This relates to functionality not present in the Base-PP and does not affect the TOE's ability to satisfy the Base-PP's SFRs.
FTP_DIT_EXT.2	This SFR defines the communication channel for Host Agents communicating with other Host Agents. This relates to functionality not present in the Base-PP and does not affect the TOE's ability to satisfy the Base-PP's SFRs.
Objective SFRs	
FMT_POL_EXT.1	This SFR defines protections for the integrity of commands sent to the Host Agent. This relates to functionality not present in the Base-PP and does not affect the TOE's ability to satisfy the Base-PP's SFRs.

Appendix A - Optional SFRs

This PP-Module does not define any optional SFRs.

Appendix B - Selection-based SFRs

FHA_CHA_EXT.1 Cache Host Agent Collected Data

This is a selection-based component. Its inclusion depends upon selection from FHA_HAD_EXT.1.1.

FHA_CHA_EXT.1.1 Absent storage space exhaustion the **Host Agent** shall cache and manage collected data for a minimum of [**assignment**: *value greater than 72*] hours on [**selection**: *persistent storage*, *non-persistent storage*] if the trusted channel is not available.

Application Note: The term *collected data* here is understood to be any type of collected endpoint data by the Host Agent destined for an enterprise security management (ESM) server. The term *manage* here is understood to be a ruleset for what is done if storage limits are reached. To meet this requirement a Host Agent must be capable of locally caching or queuing data for a minimum value that is greater than 72 hours (3 days) during periods of network dis-connectivity. In a future revision the selection of non-persistent storage will be removed.

Evaluation Activity

TSS
The evaluator shall verify the TSS details how data is cached, any rules that would effect data caching, and how cached data will be effected if storage limit are reached.
Guidance
The evalutor shall verify that any configuration options related to data caching is listed in the guidance.
Tests

- ***Test 1:*** *The evaluator shall test the Host Agents ability to cache data by disconnecting the endpoint from the network for a period of 72 hours to simulate a network connectivity failure, these should be actual hours not via changing system time. The evaluator shall exercise behaviors on the endpoint during the 72 hour time frame to generate Host Agent data. Example behaviors could be running programs, performing some authentications, installing/uninstalling software, or sample test cases provided by the vendor to generate Host Agent data. The evaluator will then reconnect the endpoint to the network and verify on the ESM system that the missing data from the 72 hour time frame is available on the ESM management portal.*

FHA_COL_EXT.1 Collected Audit

This is a selection-based component. Its inclusion depends upon selection from FHA_HAD_EXT.1.1.

FHA_COL_EXT.1.1 The Host Agent shall collect the following minimum set of endpoint event data:

a. Operating System (OS) version, architecture, and IP Address
b. Privileged and unprivileged endpoint account login activity
c. Process creation
d. Libraries and modules loaded by processes
e. Network connection activity, including destination IP
f. Files created on persistent storage
g. [**assignment**: *Other host data*]

Application Note: The intent of this requirement is to specify the minimum set of endpoint data that the Host Agent for an ESM EDR system must be capable of collecting. This requirement only applies to Host Agents used with the [EDR] PP per the selection from FHA_HAD_EXT.1. The assignment may be empty, a single item, or multiple items.

Evaluation Activity

TSS
The evaluator shall verify the TSS contains a full list of endpoint data that can be collected.
Guidance
The evaluator shall check the administrative guide and ensure that it lists all of the collectable types of endpoint event data. The evaluator shall check to make sure that every endpoint event type listed in the ST is included in the administrative guidance.
Tests
The evalutator shall run the systems causing multiple events to occur then review the items collected by the Host Agent and verify all items in the minimum set are included.

FTP_DIT_EXT.2 Protection of Data in Transit for Peer-to-Peer Host Agents

This is a selection-based component. Its inclusion depends upon selection from FDP_NET_EXT.1.1.

FTP_DIT_EXT.2.1 The Host Agent shall encrypt all transmitted data according to FPT_DIT_EXT.1 between itself and another Host Agent.

Application Note: This requirement is designed to protect the communications with other Host Agents in a peer-to-peer scenario where Host Agents are sending/receiving data from each other.

Evaluation Activity

TSS
The evaluator shall verify that the TSS contains a description of all data transmitted to other Host Agents and that all such data is protected by according to FPT_DIT_EXT.1.
Guidance
The evaluator shall ensure the guidance contains any configuration details required for ensuring data transmitted to other Host Agents is protected by TLS.
Tests

- ***Test 1:*** *The tests in FTP_DIT_EXT.1.1 shall be repeated for data trasmitted between two Host Agents.*

Appendix C - Objective SFRs

This section is reserved for requirements that are not currently prescribed by this PP-Module but are expected to be included in future versions of the PP-Module. Vendors planning on having evaluations performed against future products are encouraged to plan for these objective requirements to be met.

FMT_POL_EXT.1 Trusted Policy Update

FMT_POL_EXT.1.1 The [**selection**: *Host Agent*, *Host Agent Platform*] shall only accept policies or commands that are digitally signed in accordance with FCS_COP.1.1(3).

Application Note: The intent of this requirement is to cryptographically tie any policy updates or commends sent to the Host Agent as being from the ESM Server. This is not to protect the policies in transit as they are already protected by FTP_DIT_EXT.1.1 and/or FTP_DIT_EXT.2.1. The digital signature used to sign policies or commands must be selected in FCS_COP.1.1(3). The use of this requirement makes FCS_COP.1.1(3) from the Base-PP a mandatory requirement.

Evaluation Activity

TSS
The evaluator shall ensure that the TSS describes how the candidate policies or commands are sent to the Host Agent; the processing associated with verifying the digital signature of the policies or commands; and the actions that take place for successful (signature was verified) and unsuccessful (signature could not be verified) cases. The software components that are performing the processing must also be identified in the TSS and verified by the evaluators (this could be the Host Agent or the underlying platform).
Guidance
There is no associated guidance for this requirement.
Tests

- ***Test 1:*** *The evaluator shall perform or wait for a policy update or commands from an ESM Server to be sent to a Host Agent. The evaluator shall verify the policy or command is signed and is provided to the Host Agent. The evaluator shall verify the Host Agent accepts the digitally signed policy.*

  The execution of this test may require some configuration or a test version of either the Host Agent of the ESM system in order to view the incoming policy or command and verify that the content is digitally signed.
- ***Test 2:*** *The evaluator shall alter a policy update or command and verify the Host Agent rejects the altered policy.*

Appendix D - Extended Component Definitions

This appendix contains the definitions for the extended requirements that are used in the PP-Module including those used in Appendices A through C.

D.1 Background and Scope

This appendix provides a definition for all of the extended components introduced in this PP-Module. These components are identified in the following table:

Functional Class	Functional Components
Security Audit (FAU)	FAU_STO_EXT Audit Data Storage
Host Agent (FHA)	FHA_HAD_EXT Host Agent Declaration
Security Management (FMT)	FMT_UNR_EXT User Unenrollment Prevention
Host Agent (FHA)	FHA_CHA_EXT Cache Host Agent Collected Data FHA_COL_EXT Collected Audit
Trusted Path/Channels (FTP)	FTP_DIT_EXT Protection of Data in Transit
Security Management (FMT)	FMT_POL_EXT Trusted Policy Update

D.2 Extended Component Definitions

FAU_STO_EXT Audit Data Storage

Components in this family define requirements for the location and method of audit storage.

Component Leveling

FAU_STO_EXT.1, Audit Data Storage, requires either the TOE or its platform to store audit data using the platform's audit mechanism.

Management: FAU_STO_EXT.1

No specific management functions are identified.

Audit: FAU_STO_EXT.1

There are no auditable events foreseen.

FAU_STO_EXT.1 Audit Data Storage

Hierarchical to: No other components.

Dependencies to: No dependencies.

FAU_STO_EXT.1.1

The [**selection**: *Host Agent*, *Host Agent Platform*] shall store audit events in the platform provided logging mechanism.

FHA_HAD_EXT Host Agent Declaration

Components in this family define requirements for the ESM functionality that the TOE is compatible with.

Component Leveling

FHA_HAD_EXT.1, Host Agent Declaration, requires the TOE to be compatible with one or more types of ESM capabilities and to identify how its network communications are restricted in support of that compatibility.

Management: FHA_HAD_EXT.1

No specific management functions are identified.

Audit: FHA_HAD_EXT.1

There are no auditable events foreseen.

FHA_HAD_EXT.1 Host Agent Declaration

Hierarchical to: No other components.

Dependencies to: No dependencies.

FHA_HAD_EXT.1.1

The Host Agent shall operate with the following ESM Software:
Endpoint Detection and Response (EDR)

FMT_UNR_EXT User Unenrollment Prevention

Components in this family define requirements for ensuring that an unprivileged user cannot remove the TOE from management by another ESM component.

Component Leveling

FMT_UNR_EXT.1, User Unenrollment Prevention, requires the TSF to prevent its unenrollment by an unauthorized user.

Management: FMT_UNR_EXT.1

No specific management functions are identified.

Audit: FMT_UNR_EXT.1

There are no auditable events foreseen.

FMT_UNR_EXT.1 User Unenrollment Prevention

Hierarchical to: No other components.

Dependencies to: No dependencies.

FMT_UNR_EXT.1.1

The [**selection**: *Host Agent*, *Host Agent Platform*] shall enforce a mechanism to prevent unprivileged users of the platform from unenrolling the Host Agent with the ESM system.

FHA_CHA_EXT Cache Host Agent Collected Data

Components in this family define requirements for the location and duration of storage for its collected data.

Component Leveling

FHA_CHA_EXT.1, Cache Host Agent Collected Data, requires either the TOE or its platform to store audit data using the platform's logging mechanism.

Management: FHA_CHA_EXT.1

No specific management functions are identified.

Audit: FHA_CHA_EXT.1

There are no auditable events foreseen.

FHA_CHA_EXT.1 Cache Host Agent Collected Data

Hierarchical to: No other components.

Dependencies to: FHA_COL_EXT.1 Collected Audit
FHA_HAD_EXT.1 Host Agent Declaration

FHA_CHA_EXT.1.1

Absent storage space exhaustion the **Host Agent** shall cache and manage collected data for a minimum of [**assignment**: *value greater than 72*] hours on [**selection**: *persistent storage*, *non-persistent storage*] if the trusted channel is not available.

FHA_COL_EXT Collected Audit

Components in this family define requirements for the collection of data theTOE collects from its operational environment as audit data.

Component Leveling

FHA_COL_EXT.1, Collected Audit, requires the TOE to collect a specified set of data from its operational environment.

Management: FHA_COL_EXT.1

No specific management functions are identified.

Audit: FHA_COL_EXT.1

There are no auditable events foreseen.

FHA_COL_EXT.1 Collected Audit

Hierarchical to: No other components.

Dependencies to: FHA_HAD_EXT.1 Host Agent Declaration

FHA_COL_EXT.1.1

The Host Agent shall collect the following minimum set of endpoint event data:

a. Operating System (OS) version, architecture, and IP Address

b. Privileged and unprivileged endpoint account login activity
c. Process creation
d. Libraries and modules loaded by processes
e. Network connection activity, including destination IP
f. Files created on persistent storage
g. [**assignment**: *Other host data*]

FTP_DIT_EXT Protection of Data in Transit

This family is defined in the [AppPP]. This PP-Module adds a component to the existing family definition.

Component Leveling

FTP_DIT_EXT.2, Protection of Data in Transit for Peer-to-Peer Host Agents, requires the TSF to secure data in transit between itself and another ESM Host Agent using TLS.

Management: FTP_DIT_EXT.2

No specific management functions are identified.

Audit: FTP_DIT_EXT.2

There are no auditable events foreseen.

FTP_DIT_EXT.2 Protection of Data in Transit for Peer-to-Peer Host Agents

Hierarchical to: No other components.

Dependencies to: FCS_TLS_EXT.1 TLS Protocol
[FCS_TLSC_EXT.1 TLS Client Protocol OR
FCS_TLSS_EXT.1 TLS Server Protocol]
FHA_HAD_EXT.1 Host Agent Declaration

FTP_DIT_EXT.2.1

The Host Agent shall encrypt all transmitted data according to FPT_DIT_EXT.1 between itself and another Host Agent.

FMT_POL_EXT Trusted Policy Update

Components in this family define requirements for the TOE's verification of policies or commands transmitted to it.

Component Leveling

FMT_POL_EXT.1, Trusted Policy Update, requires the TSF to reject any unsigned management policies or commands sent to it.

Management: FMT_POL_EXT.1

No specific management functions are identified.

Audit: FMT_POL_EXT.1

There are no auditable events foreseen.

FMT_POL_EXT.1 Trusted Policy Update

Hierarchical to: No other components.

Dependencies to: FCS_COP.1 Cryptographic Operation

FMT_POL_EXT.1.1

The [**selection**: *Host Agent*, *Host Agent Platform*] shall only accept policies or commands that are digitally signed in accordance with FCS_COP.1.1(3).

Appendix E - Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • 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.
[AppPP]	Protection Profile for Application Software
[EDR]	Protection Profile for Endpoint Detection and Response

Appendix F - Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
ASLR	Address Space Layout Randomization
CC	Common Criteria
CEM	Common Evaluation Methodology
CESG	Communications-Electronics Security Group
CMC	Certificate Management over CMS
CMS	Cryptographic Message Syntax
CN	Common Names
CRL	Certificate Revocation List
CSA	Computer Security Act
DEP	Data Execution Prevention
DES	Data Encryption Standard
DHE	Diffie-Hellman Ephemeral
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
DT	Date/Time Vector
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standards
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier

OMB	Office of Management and Budget
OS	Operating System
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PP	Protection Profile
PP	Protection Profile
PP-Module	Protection Profile Module
RBG	Random Bit Generator
RFC	Request for Comment
RNG	Random Number Generator
RNGVS	Random Number Generator Validation System
S/MIME	Secure/Multi-purpose Internet Mail Extensions
SAN	Subject Alternative Name
SAR	Security Assurance Requirement
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
ST	Security Target
SWID	Software Identification
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
XCCDF	eXtensible Configuration Checklist Description Format
XOR	Exclusive Or