PP-Module for Host Agent

Version: 1.0

2020-10-23

National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2020-10-23	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 PP-Module is intended for use with the following Base-PPs:

- Protection Profile for Application Software [AppPP], Version 1.3.

This Base-PP is valid because a Host Agent is deployed as a software application on a general-purpose operating 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 TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Common Criteria (CC)	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 (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	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 (PP-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 an 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 (ESM)	A type of 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.
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 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

The requirements for the EDR are not covered in this PP-Module, however it is expected that an ESM system will evaluate against a PP-Configuration that includes both the [EDR] PP-Module and the Host AgentPP-Module. The EDR PP-Module covers the security functionality needed on the server or cloud service, and the paired Host Agent PP-Module covers the security functionality needed on the endpoint device (desktop, mobile device, etc.). At this time only the [EDR] PP-Module is published and ready for use with this Host Agent PP-Module. Future versions of this PP-Module will include requirements for other classes of ESM software.

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 PP-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.

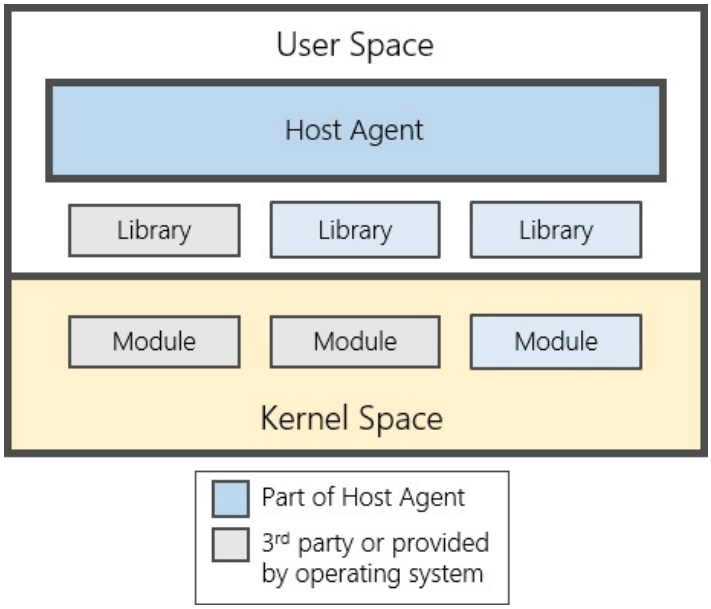

Figure 1: Sample Host Agent TOE

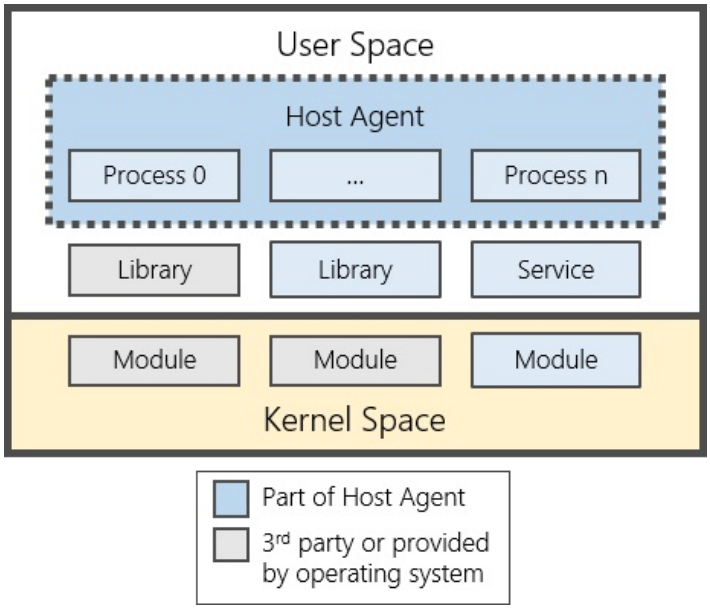

Figure 2: Sample Host Agent TOE

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 PP-Module are designed to address the security problem for the following use cases. These use cases are intentionally very broad, as many different types of ESM Host Agent products may exist. As this PP-Module is revised to allow for more specific types of ESM Host Agent products, additional use cases may be devised.

[USE CASE 1] Communication

The Host Agent allows for communication interactively or non-interactively with other 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

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

The following PPs and PP-Modules are allowed to be specified in a PP-Configuration with this PP-Module:

- PP-Module for Endpoint Detection and Response (EDR), Version 1.0.

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

This PP-Module 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. These extend any threats, assumptions, and organizational security policies defined by the Base-PP.

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 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

This PP-Module does not define any assumptions.

This PP-Module defines no additional assumptions beyond those defined in the Base-PP.

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/HA, FAU_STO_EXT.1

O.DATA_RECORDER
Conformant Host Agents will collect security-relevant data from a target entity in the Operational Environment and transmit it to a trusted entity for further processing. They will also implement mechanisms to ensure that collected data is retained in the event that the trusted channel is unavailable to prevent data loss.

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

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_UNR_EXT.1, FMT_POL_EXT.1 (objective)

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

Addressed by: FMT_SMF.1/HA

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 PP-Module does not define any objectives for the Operational 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.
	O.HA_MANAGEMENT	The threat T.DATA_LOSS is countered by O.HA_MANAGEMENT as this provides for the management of sending data and tracking of enrolled hosts.
T.TAMPER	O.ACCOUNTABILITY	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.I
	O.INTEGRITY	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 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 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

This PP-Module does not modify any SFRs defined by the App 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/HA Audit Data Generation

FAU_GEN.1.1/HA

Refinement: The **Host Agent** shall generate an audit record of the following auditable events:

a. ~~Start-up and shutdown of the audit functions;~~
b. All auditable events for the [*not specified*] level of audit; and

[

a. Change in enrollment state with an ESM system,
*b. [**selection**: Receiving, Generating] periodic heartbeat events,*
*c. [**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. Changes in enrollment include new enrollment and unenrollment.

FAU_GEN.1.2/HA

Refinement: 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. Outcome (success or failure) of the event,
e. For each audit type, based on the auditable event definitions of the functional components included in the PP/ST, [**assignment**: *Other audit relevant information*].

Application Note: All audits must contain at least the information mentioned in

FAU_GEN.1.2/HA, 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 contain 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/HA. If the job of this Host Agent is to generate or collect events for an ESM 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
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 User Data Protection

FDP_NET_EXT.2 Network Communications

FDP_NET_EXT.2.1

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 evaluator shall confirm the TSS lists network communication destinations and that it matches the selections made in the SFR.

Guidance
The evaluator shall confirm that guidance is provided for any configuartion needed to limit network communications.

Tests
The evaluator shall run the application. While the application is running, the evaluator shall sniff network traffic ignoring all non-application associated traffic and verify that any network communications witnessed are limited to the selection made in the SFR.

5.2.3 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: [**selection**:

- *Endpoint Detection and Response (EDR),*
- *[**assignment**: Other NIAP-approved ESM servers]*

].

Application Note: Currently, the only NIAP-approved ESM server is EDR; PP-Modules for other ESM servers (Systems Management and Audit Server) will be added in the future. By including EDR, the additional FHA_CHA_EXT.1 and FHA_COL_EXT.1 requirements must 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 guidance exists for enrollment with all compatible ESM products identified in the ST.

Tests
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.

5.2.4 Security Management (FMT)

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

FMT_SMF.1.1/HA

The **Host Agent** shall be capable of performing the following management functions:

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

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.

Chart legend: X = Mandatory

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
The evaluator shall test the ability to configure the Host Agent and test each function listed in the SFR. 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 are no guidance EAs for this component.

Tests
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.

5.3 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:

OBJECTIVE	ADDRESSED BY	RATIONALE
O.ACCOUNTABILITY	FAU_GEN.1/HA, FAU_STO_EXT.1	The PP-Module includes FAU_GEN.1/HA to ensure that the TOE provides accountability through the generation of audit records for security-relevant events. The PP-Module includes FAU_STO_EXT.1 to ensure that the TOE provides accountability by ensuring that audit records are stored using an appropriate mechanism.
O.DATA_RECORDER	FHA_CHA_EXT.1 (selection-based), FHA_COL_EXT.1 (selection-based), FHA_HAD_EXT.1	The PP-Module includes FHA_HAD_EXT.1 to define the interface between the Host Agent and the intended destination for the data it transmits. The PP-Module includes FHA_CHA_EXT.1 to define the

		ability of the Host Agent to maintain collected data during periods of communications outage. The PP-Module includes FHA_COL_EXT.1 to define the data that the Host Agent can collect from its Operational Environment.
O.INTEGRITY	FMT_POL_EXT.1 (objective), FMT_UNR_EXT.1	The PP-Module includes FMT_UNR_EXT.1 to ensure that the Host Agent is protected from unenrollment actions that would result in it being unable to receive or enforce policy and/or commands sent to it. The PP-Module includes FMT_POL_EXT.1 to optionally ensure that policy and/or command data sent to the Host Agent has its integrity proven with a verifiable digital signature before being accepted.
O.HA_MANAGEMENT	FMT_SMF.1/HA	The PP-Module includes FMT_SMF.1/HA to define the management functions that are configurable on the Host Agent.
O.PROTECTED_COMMS	FTP_DIT_EXT.1 (from Base-PP), FTP_DIT_EXT.2 (selection-based)	The PP-Module includes FTP_DIT_EXT.1 by reference to show that the Host Agent is capable of using a trusted channel defined by the Base-PP for its own specific use. The PP-Module includes FTP_DIT_EXT.2 to optionally define the trusted communications channel between multiple Host Agents.

6 Consistency Rationale

6.1 Protection Profile for Application Software

6.1.1 Consistency of TOE Type

If this PP-Module is used to extend the Application Software PP, 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, assumptions, and OSPs defined by this PP-Module (see section 3.1) supplement those defined in the App PP as follows:

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.DATA_LOSS	This threat is consistent with the Base-PP because a lack of network availability could be a specific consequence of the T.NETWORK_ATTACK threat.
T.TAMPER	This threat is consistent with the Base-PP because tampering with the application is a specific example of the T.LOCAL_ATTACK threat.

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 that relate to the specific functionality described by the PP-Module and further satisfy the objective.
O.HA_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 that relate to the specific functionality described by the PP-Module and further satisfy the objective.
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 that relate to the specific functionality described by the PP-Module and further satisfy the objective.

This PP-Module does not define any objectives for the TOE'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 PPis being used for its intended purpose. 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	
This PP-Module does not modify any requirements when the App PP is the base.	
Mandatory SFRs	
FAU_GEN.1/HA	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.
FDP_NET_EXT.2	The Base-PP does not define specific network communications for EDR - HA communications. 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/HA	This SFR defines management functions for the SFRs defined in this PP-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

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 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 affect data caching, and how cached data will be affected if storage limits are reached.

Guidance
The evalutor shall verify that any configuration options related to data caching are listed in the guidance.

Tests
The evaluator shall test the Host Agent's 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

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-Module 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 evaluator shall run the systems causing multiple events to occur and then review the items collected by the Host Agent to verify that all items in the minimum set are included.

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

FTP_DIT_EXT.2.1

The Host Agent shall [**selection**: *encrypt, invoke platform-provided functionality to encrypt*] all transmitted data according to FTP_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. The selection of whether the TSF of the TOE platform encrypts these communications should be consistent with any selections made in FTP_DIT_EXT.1

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 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 according to FPT_DIT_EXT.1.

Tests
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 using [**selection**: *RSA, ECDSA*] signatures that meet FIPS PUB 186-4.

Application Note: The intent of this requirement is to cryptographically tie any policy updates or commands 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_ITC.1 (in the [EDR] PP-Module) and/or FTP_DIT_EXT.2.1. If the TSF implements this function, any signature algorithms used should be consistent with any selections made in FCS_COP.1(3).

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 are no guidance EAs for this component.

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_CHA_EXT Cache Host Agent Collected Data FHA_COL_EXT Collected Audit FHA_HAD_EXT Host Agent Declaration
Security Management (FMT)	FMT_POL_EXT Trusted Policy Update FMT_UNR_EXT User Unenrollment Prevention
Trusted Path/Channels (FTP)	FTP_DIT_EXT Protection of Data in Transit

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: [**selection**:

- *Endpoint Detection and Response (EDR),*
- *[**assignment**: Other NIAP-approved ESM servers]*

].

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 the TOE 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 a TSF-provided or platform-provided trusted channel.

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: FHA_HAD_EXT.1 Host Agent Declaration
FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.2.1

The Host Agent shall [**selection**: *encrypt*, *invoke platform-provided functionality to encrypt*] all transmitted data according to FTP_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 using [**selection**: *RSA*, *ECDSA*] signatures that meet FIPS PUB 186-4.

Appendix E - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this Protection Profile. However, these requirements are not featured explicitly as SFRs and should not be included in the ST. They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, **8.2 Dependencies between components**.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the Protection Profile provides evidence that these controls are present and have been evaluated.

Requirement	Rationale for Satisfaction
FPT_STM.1 - Reliable Time Stamps	CC Part 2 specifies FPT_STM.1 as a dependency of FAU_GEN.1 because the audit records require a reliable timestamp to satisfy FAU_GEN.1.2. This dependency is implicitly addressed through the A.PLATFORM assumption of the Base-PP because a "trustworthy computing platform" is assumed to include a reliable system clock.

Appendix F - 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, Version 1.3, March 1, 2019
[EDR]	PP-Module for Endpoint Detection and Response, Version 1.0, October 23rd. 2020

Appendix G - Acronyms

Acronym	Meaning
API	Application Programming Interface
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
EA	Evaluation Activity
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standards
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
RSA	Rivest, Shamir, Adleman (digital signature algorithm)
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification