PP-Module for Host Agent

Version: 2.0
2026-01-13
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2020-10-23	First version released
2.0	2026-01-13	CC:2022 Conversion

Contents

1 Introduction
1.1 Overview
1.2 Terms
1.2.1 Common Criteria Terms
1.2.2 Technical Terms
1.3 Compliant Targets of Evaluation
1.3.1 TOE Boundary
1.3.2 TOE Platform
1.4 Use Cases
2 Conformance Claims
3 Security Problem Definition
3.1 Threats
3.2 Assumptions
3.3 Organizational Security Policies
4 Security Objectives
4.1 Security Objectives for the Operational Environment
5 Security Requirements
5.1 Protection Profile for Application Software Security Functional Requirements Direction
5.1.1 Modified SFRs
5.2 TOE Security Functional Requirements
5.2.1 Auditable Events for Mandatory SFRs
5.2.2 Security Audit (FAU)
5.2.3 User Data Protection (FDP)
5.2.4 Host Agent (FHA)
5.2.5 Security Management (FMT)
5.3 TOE Security Functional Requirements Rationale
6 Consistency Rationale
6.1 Protection Profile for Application Software
6.1.1 Consistency of TOE Type
6.1.2 Consistency of Security Problem Definition
6.1.3 Consistency of OE Objectives
6.1.4 Consistency of Requirements
Appendix A - Optional SFRs
A.1 Strictly Optional Requirements
A.2 Objective Requirements
A.2.1 Auditable Events for Objective SFRs
A.2.2 Security Management (FMT)
A.3 Implementation-dependent Requirements
Appendix B - Selection-based Requirements
B.1 Auditable Events for Selection-based SFRs
B.2 Host Agent (FHA)
B.3 Trusted Path/Channels (FTP)
Appendix C - Extended Component Definitions
C.1 Extended Components Table
C.2 Extended Component Definitions
C.2.1 Host Agent (FHA)
C.2.1.1 FHA_CHA_EXT Cache Host Agent Collected Data
C.2.1.2 FHA_COL_EXT Collected Audit
C.2.2 Security Audit (FAU)
C.2.2.1 FAU_STO_EXT Audit Data Storage
C.2.3 Security Management (FMT)
C.2.3.1 FMT_UNR_EXT User Unenrollment Prevention
C.2.3.2 FMT_POL_EXT Trusted Policy Update
C.2.4 Trusted Path/Channels (FTP)

C.2.4.1 FTP_DIT_EXT Protection of Data in Transit
C.2.5 User Data Protection (FDP)
C.2.5.1 FDP_NET_EXT Network Communications
Appendix D - Implicitly Satisfied Requirements
Appendix E - Acronyms
Appendix F - Bibliography

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 Version 2.0

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.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
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.
Direct Rationale	A type of Protection Profile, PP-Module, or Security Target in which the security problem definition (SPD) elements are mapped directly to the SFRs and possibly to the security objectives for the operational environment. There are no security objectives for the TOE.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Extended Package (EP)	A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
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-PPs.
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.

Target of Evaluation (TOE)	The product under evaluation.
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.

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 PP-Module for Host Agent covers the security functionality needed on the endpoint device (desktop, mobile device, etc.) for ESM software products in general. This version of the PP-Module is paired with the PP-Module for EDR. Future versions of this PP-Module will include requirements for other classes of ESM software. It is expected that an ESM system will evaluate against a PP-Configuration that includes both the PP-Module for Host Agent and at least one other ESM PP-Module; currently, this only includes the PP-Module for EDR.

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.

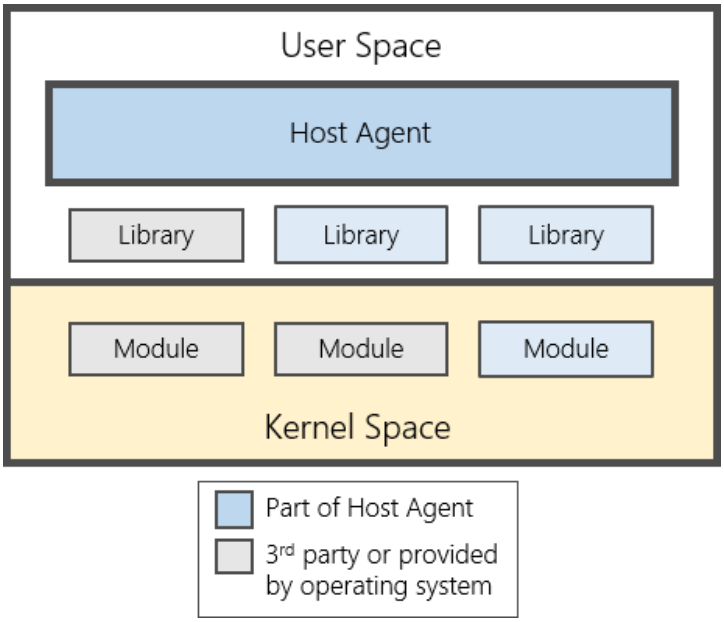


Figure 1: Sample Host Agent TOE

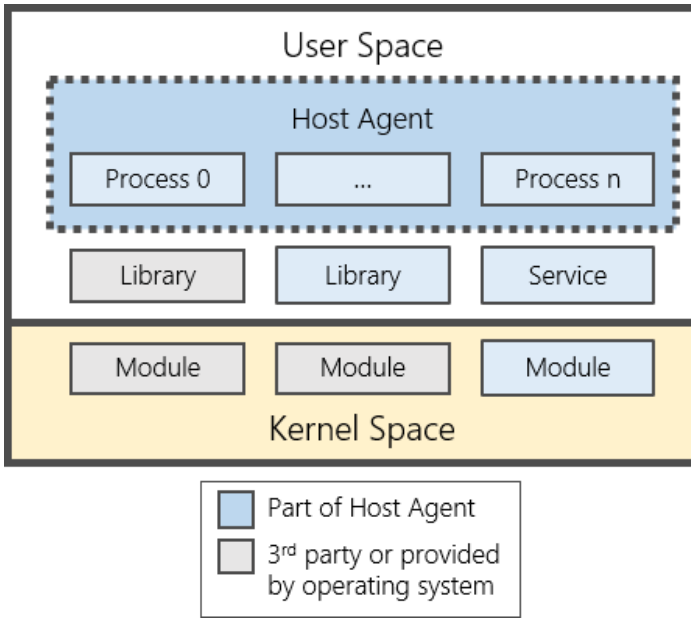


Figure 2: Sample Host Agent TOE

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

Conformance Statement

An ST must claim exact conformance to this PP-Module.

The evaluation methods used for evaluating the TOE are a combination of the workunits defined in [CEM] as well as the Evaluation Activities for ensuring that individual SFRs and SARs have a sufficient level of supporting evidence in the Security Target and guidance documentation and have been sufficiently tested by the laboratory as part of completing ATE_IND.1. Any functional packages this PP claims similarly contain their own Evaluation Activities that are used in this same manner.

CC Conformance Claims

This PP-Module is conformant to Part 2 (extended) and Part 3 (extended) of Common Criteria CC:2022, Revision 1.

PP Claim

This PP-Module does not claim conformance to any Protection Profile.

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

- Protection Profile for Application Software Version 2.0
- PP-Module for Endpoint Detection and Response (EDR), Version 2.0
- PP-Module for Enterprise-Management (EM), Version 2.0

Package Claim

- This PP-Module is Functional Package for SSH, Version 2.0 conformant.
- This PP-Module is Functional Package for TLS, Version 2.1 conformant.
- This PP-Module is Functional Package for X.509, Version 1.0 conformant.
- This PP-Module does not conform to any assurance packages.

The functional packages to which the PP conforms may include SFRs that are not mandatory to claim for the sake of conformance. An ST that claims one or more of these functional packages may include any non-mandatory SFRs that are appropriate to claim based on the capabilities of the TSF and on any triggers for their inclusion based inherently on the SFR selections made.

3 Security Problem Definition

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 document does not define any additional assumptions.

3.3 Organizational Security Policies

An organization deploying the TOE is expected to satisfy the organizational security policy listed below in addition to all organizational security policies defined by the claimed Base-PP.

This document does not define any additional OSPs.

4 Security Objectives

4.1 Security Objectives for the Operational Environment

This PP-Module does not define any objectives for the OE.

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 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 Protection Profile for Application Software 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 Auditable Events for Mandatory SFRs

Table 1: Auditable Events for Mandatory Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1/HA	No events specified	N/A
FAU_STO_EXT.1	No events specified	N/A
FDP_NET_EXT.2	No events specified	N/A
FHA_HAD_EXT.1	No events specified	N/A
FMT_SMF.1/HA	No events specified	N/A
FMT_UNR_EXT.1	No events specified	N/A

5.2.2 Security Audit (FAU)

FAU_GEN.1/HA Audit Data Generation

FAU_GEN.1.1/HA

The TSF shall be able to generate audit data 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;

[

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

The **[selection: *TSF*, *TOE Platform*]** shall record within the audit data at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
b. For each audit type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package, or 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.

FAU_STO_EXT.1 Audit Data Storage

FAU_STO_EXT.1.1

The [**selection**: *TSF*, *TOE 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.

5.2.3 User Data Protection (FDP)

FDP_NET_EXT.2 Network Communications

FDP_NET_EXT.2.1

The TSF 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.

5.2.4 Host Agent (FHA)

FHA_HAD_EXT.1 Host Agent Declaration

FHA_HAD_EXT.1.1

The TSF 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.

5.2.5 Security Management (FMT)

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

FMT_SMF.1.1/HA

The TSF shall be capable of performing the following management functions: [**assignment**: *list of management functions to be provided by the TSF*].

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.

FMT_UNR_EXT.1 User Unenrollment Prevention

FMT_UNR_EXT.1.1

The [**selection**: *TSF*, *TOE 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.

5.3 TOE Security Functional Requirements Rationale

The following rationale provides justification for each SFR for the TOE, showing that the SFRs are suitable to address the specified threats:

Table 2: SFR Rationale

Threat	Addressed by	Rationale
T.DATA_LOSS	FDP_NET_EXT.2	The PP-Module includes FDP_NET_EXT.2 to define the trust network connection to another host.
	FHA_CHA_EXT.1 (selection-based)	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.
	FHA_COL_EXT.1 (selection-based)	The PP-Module includes FHA_COL_EXT.1 to define the data that the Host Agent can collect from its Operational Environment.
	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
	FMT_SMF.1/HA	The PP-Module includes FMT_SMF.1/HA to define the management functions that are configurable on the Host Agent.
	FTP_DIT_EXT.2 (selection-based)	The PP-Module includes FTP_DIT_EXT.2 to optionally define the trusted communications channel between multiple Host Agents.
T.TAMPER	FAU_GEN.1/HA	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.
	FAU_STO_EXT.1	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.
	FMT_POL_EXT.1 (objective)	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.
	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.

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

Table 3: Consistency of Security Problem Definition (App PP base)

PP-Module Threat, Assumption, OSP	Consistency Rationale
T.DATA_LOSS	This threat relates to the loss of data that is collected by the ESM 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 OE Objectives

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 PP is 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:

Table 4: Consistency of Requirements (App PP base)

PP-Module Requirement	Consistency Rationale
	Modified SFRs
	This PP-Module does not modify any requirements when the App PP is the base.
	Additional SFRs
	This PP-Module does not add 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.	
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.
Implementation-dependent SFRs	
This PP-Module does not define any Implementation-dependent 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.

Appendix A - Optional SFRs

A.1 Strictly Optional Requirements

This PP-Module does not define any Strictly Optional SFRs or SARs.

A.2 Objective Requirements

A.2.1 Auditable Events for Objective SFRs

Table 5: Auditable Events for Objective Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FMT_POL_EXT.1	No events specified	N/A

A.2.2 Security Management (FMT)

FMT_POL_EXT.1 Trusted Policy Update

FMT_POL_EXT.1.1

The [**selection**: *TSF*, *TOE Platform*] shall only accept policies or commands that are digitally signed using [**selection**: *RSA*, *ECDSA*] signatures that meet FIPS PUB 186-5.

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 PP-Module for EDR, FTP_DIT_EXT.2.1, or both. If the TSF implements this function, any signature algorithms used should be consistent with any selections made in FCS_COP.1/SigGen and FCS_COP.1/SigVer in the Protection Profile for Application Software, Version 2.0.

A.3 Implementation-dependent Requirements

This PP-Module does not define any Implementation-dependent SFRs.

Appendix B - Selection-based Requirements

B.1 Auditable Events for Selection-based SFRs

Table 6: Auditable Events for Selection-based Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FHA_CHA_EXT.1	No events specified	N/A
FHA_COL_EXT.1	No events specified	N/A
FTP_DIT_EXT.2	No events specified	N/A

B.2 Host Agent (FHA)

FHA_CHA_EXT.1 Cache Host Agent Collected Data

FHA_CHA_EXT.1.1

The TSF shall cache collected data up to [**assignment**: *size of cache storage capacity*] 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 ST author specifies the size of the cache storage and whether it is implemented in persistent or non-persistent storage.

FHA_CHA_EXT.1.2

The TSF shall [**selection**: *overwrite previous data according to the following rule: [**assignment**: rule for overwriting previously cached data]*, *[**assignment**: other actions]*] when the local cache is full.

Application Note: This requirement addresses how the Host Agent handles collected data while the trusted path is not available and the local cache is full.

FHA_COL_EXT.1 Collected Audit

FHA_COL_EXT.1.1

The TSF 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.

B.3 Trusted Path/Channels (FTP)

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

FTP_DIT_EXT.2.1

The TSF 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 and 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

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-Module are listed in this table:

Table 7: Extended Component Definitions

Functional Class	Functional Components
Host Agent (FHA)	FHA_CHA_EXT Cache Host Agent Collected Data FHA_COL_EXT Collected Audit
Security Audit (FAU)	FAU_STO_EXT Audit Data Storage
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
User Data Protection (FDP)	FDP_NET_EXT Network Communications

C.2 Extended Component Definitions

C.2.1 Host Agent (FHA)

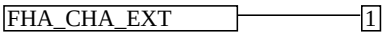
This PP-Module defines the following extended components as part of the FHA class originally defined by CC Part 2:

C.2.1.1 FHA_CHA_EXT Cache Host Agent Collected Data

Family Behavior

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

The TSF shall cache collected data up to [**assignment**: *size of cache storage capacity*] on [**selection**: *persistent storage, non-persistent storage*] if the trusted channel is not available.

FHA_CHA_EXT.1.2

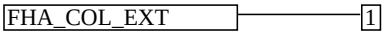
The TSF shall [**selection**: *overwrite previous data according to the following rule: [**assignment**: rule for overwriting previously cached data], [**assignment**: other actions]*] when the local cache is full.

C.2.1.2 FHA_COL_EXT Collected Audit

Family Behavior

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 TSF 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*].

C.2.2 Security Audit (FAU)

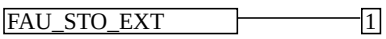
This PP-Module defines the following extended components as part of the FAU class originally defined by CC Part 2:

C.2.2.1 FAU_STO_EXT Audit Data Storage

Family Behavior

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**: *TSF*, *TOE Platform*] shall store audit events in the platform-provided logging mechanism.

C.2.3 Security Management (FMT)

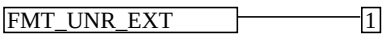
This PP-Module defines the following extended components as part of the FMT class originally defined by CC Part 2:

C.2.3.1 FMT_UNR_EXT User Unenrollment Prevention

Family Behavior

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

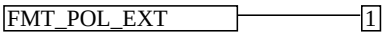
The [**selection**: *TSF*, *TOE Platform*] shall enforce a mechanism to prevent unprivileged users of the platform from unenrolling the Host Agent with the ESM system.

C.2.3.2 FMT_POL_EXT Trusted Policy Update

Family Behavior

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**: *TSF*, *TOE Platform*] shall only accept policies or commands that are digitally signed using [**selection**: *RSA*, *ECDSA*] signatures that meet FIPS PUB 186-5.

C.2.4 Trusted Path/Channels (FTP)

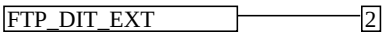
This PP-Module defines the following extended components as part of the FTP class originally defined by CC Part 2:

C.2.4.1 FTP_DIT_EXT Protection of Data in Transit

Family Behavior

This family is defined in the. 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:	FDN_NET_EXT.2 Network Communications
	FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.2.1

The TSF shall [**selection**: *encrypt*, *invoke platform-provided functionality to encrypt*] all transmitted data according to FTP_DIT_EXT.1 between itself and another Host Agent.

C.2.5 User Data Protection (FDP)

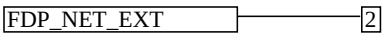
This PP-Module defines the following extended components as part of the FDP class originally defined by CC Part 2:

C.2.5.1 FDP_NET_EXT Network Communications

Family Behavior

Components in this family define requirements for recording the occurrence of security relevant events.

Component Leveling



FDP_NET_EXT.2, Network Communications, requires either the TSF restrict network communications.

Management: FDP_NET_EXT.2

There are no management functions foreseen.

Audit: FDP_NET_EXT.2

There are no audit events foreseen.

FDP_NET_EXT.2 Network Communications

Hierarchical to:	No other components.
Dependencies to:	No dependencies.

FDP_NET_EXT.2.1

The TSF shall restrict network communications to: [**selection**:

- *An ESM server*
- *Another Host Agent*

]

Appendix D - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP-Module. 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, 8.3 Dependencies between components.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the PP-Module 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 E - Acronyms

Table 8: Acronyms

Acronym	Meaning
API	Application Programming Interface
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
EA	Evaluation Activity
ECDSA	Elliptic Curve Digital Signature Algorithm
EDR	Endpoint Detection and Response
EP	Extended Package
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standards
FP	Functional Package
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
TSFI	TSF Interface
TSS	TOE Summary Specification

Appendix F - Bibliography

Table 9: Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and general model, CCMB-2022-11-001, CC:2022, Revision 1, November 2022. • Part 2: Security functional requirements, CCMB-2022-11-002, CC:2022, Revision 1, November 2022. • Part 3: Security assurance requirements, CCMB-2022-11-003, CC:2022, Revision 1, November 2022. • Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022, Revision 1, November 2022. • Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005, CC:2022, Revision 1, November 2022.
[CEM]	Common Methodology for Information Technology Security Evaluation - • Evaluation methodology, CCMB-2022-11-006, CC:2022, Revision 1, November 2022.
[AppPP]	Protection Profile for Application Software, Version 2.0, June 16, 2025
[EDR]	PP-Module for Endpoint Detection and Response, Version 2.0, January 13, 2026