Illumio Adaptive Security Platform Security Target

Version v1.3
July 9, 2019

Prepared For:

160 San Gabriel Drive
Sunnyvale, CA 94086

Evaluated By:

Revision History

Date	Version	Description
2/2/2018	0.1	Initial draft outlining evaluated TOE functionality
2/12/2018	0.2	Finalizing SFR selections and assignments
2/22/2018	0.3	Finalizing TSS section based on discussions with Illumio
5/5/2018	0.4	Editorial changes based on vendor review and initial product testing
7/12/2018	0.5	Changes to the TOE boundary based on Scheme comments
7/17/2018	0.6	Addressing ASE OR
7/27/2018	0.7	Addressing follow-up comments
8/3/2018	0.8	Addressing additional Scheme comments
3/8/2019	0.9	Finalizing ST for check-out
4/29/2019	1.0	Clarifying policy identifiers to address observation
5/14/2019	1.1	Updating final build numbers
5/28/2019	1.2	Minor comments
7/9/2019	1.3	Addressing additional Scheme comments

Table of Contents

Figures and Tables

1 Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization.

The TOE is Illumio Adaptive Security Platform v18.2.2, or ASP, which is a policy management product designed to manage access control policy within an enterprise environment.

1.1 *Security Target Reference*

ST Title: Illumio Adaptive Security Platform Security Target

ST Version: v1.3

ST Author: CygnaCom Solutions Inc.

ST Date: July 9, 2019

1.2 *TOE Reference*

TOE Developer: *Illumio*

Evaluation Sponsor: *Illumio*

TOE Identification: *Illumio Adaptive Security Platform v18.2.2*

Table 1-1: TOE Platforms

Series	Supported Platforms
Illumio Adaptive Security Platform (ASP) v18.2.2	
Policy Compute Engine (PCE) v18.2.2-13462	Red Hat Enterprise Linux 7.4 running on Intel Core i7 with AES-NI
	Red Hat Enterprise Linux 7.4 running on Intel Core i5 with AES-NI
	Red Hat Enterprise Linux 7.4 running on Intel Xeon E5 with AES-NI
Virtual Enforcement Node (VEN) v18.2.2-4339	Windows Server 2016 running on Intel Xeon E5 with AES-NI
	Windows Server 2012 R2 Intel Xeon E5 with AES-NI

CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.
Assurance Level:	Protection Profile Conformant

1.3 *TOE Product Type*

The Target of Evaluation (TOE), Illumio Adaptive Security Platform v18.2.2, or ASP, is an Enterprise Security Management Policy Management (ESM PM) product. The TOE is a software application used in the enterprise setting to map and manage communications within, and across, tiers of applications by defining access control policy.

1.4 *TOE Security Functionality*

- Enterprise Security Management
  - Enterprise authentication
  - Policy definition and transmission
- Security Audit
  - Audit of security-relevant events
  - Secure logging to a remote audit server
- Cryptographic Support
  - Platform-implemented TLS secure channels
- Identification and Authentication
  - Authentication failure handling
- Security Management
  - Role-based access control
- Protection of the TOE Security Function (TSF)
  - Protection of stored credentials
  - Protection of secret key parameters
- TOE Access
  - Access banner
  - Session timeouts
- Trusted Path/Channels
  - Secure channel for remote administration
  - Secure channel with authorized IT entities

As with all evaluations claiming conformance to a standard Protection Profile (PP), the evaluated security functionality is both determined by and tailored to specific component and configuration requirements dictated by exact conformance to the PP. A detailed description of the evaluated security functionality can be found in the TOE Summary Specification section of this document.

2 Conformance Claims

2.1 *Common Criteria Conformance Claim*

This Security Target [ST] and the Target of Evaluation [TOE] are conformant to the following Common Criteria [CC] specifications:

- *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-002*
    - Part 2 Extended
- *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 4, September 2012, CCMB-2012-09-003*
    - Part 3 Conformant

2.2 *Protection Profile Claim*

The TOE claims *exact* conformance to *Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1, October 24, 2013* [ESM PM PP].

2.3 *Package Claim*

The TOE does not claim to be conformant with any pre-defined packages.

2.4 *Conformance Rationale*

This Security Target (ST) claims exact conformance to only one Protection Profile – the ESM PM PP.

The security problem definition of this ST is consistent with the statement of the security problem definition in the PP, as the ST claims *exact* conformance to the PP and no other threats, organizational security policies, or assumptions are added.

The security objectives of this ST are consistent with the statement of the security objectives in the PP as the ST claims *exact* conformance to the PP and no other security objectives are added.

The security requirements of this ST are consistent with the statement of the security requirements in the PP as the ST claims *exact* conformance to the PP.

2.5 *Relevant Technical Decisions*

- TD0320 – TLS ciphers in ESM PPs
    - Removal of mandatory ciphersuites

  - Applied
- TD0245 – Updates to FTP_ITC and FTP_TRP for ESM PPs
  - Mandatory inclusion of protocol SFRs in the ST
  - Applied
- TD0079 – RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
  - Removal of ANS X9.31
  - Not applicable to the evaluation, FCS_RBG_EXT.1 not claimed
- TD0071 – Use of SHA-512 in ESM PPs
  - Added SHA-512 algorithm to FCS_COP.1 selections
  - Not applicable to the evaluation, FCS_COP.1 not claimed
- TD0066 – Clarification of FAU_STG_EXT.1 Requirement in ESM PPs
  - External audit reconciliation clarified as optional
  - Applied
- TD0055 – Move FTA_TAB.1 to Selection-Based Requirement
  - Inclusion of FTA_TAB.1 is conditional;
- TD0042 – Removal of Low-level Crypto Failure Audit from PPs
  - Removal of audit events for FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(*), FCS_RBG_EXT.1
  - Not applicable to the evaluation, SFRs not claimed

3 TOE Description

The TOE, Illumio Adaptive Security Platform v18.2.2, or ASP, is an enterprise policy management product. The TOE's primary purpose is to manage communications within, and across, tiers of applications by defining access control policy. The TOE is a distributed software application that consists of the Policy Compute Engine (PCE) and the Virtual Enforcement Node (VEN).

3.1 *TOE Overview and Usage*

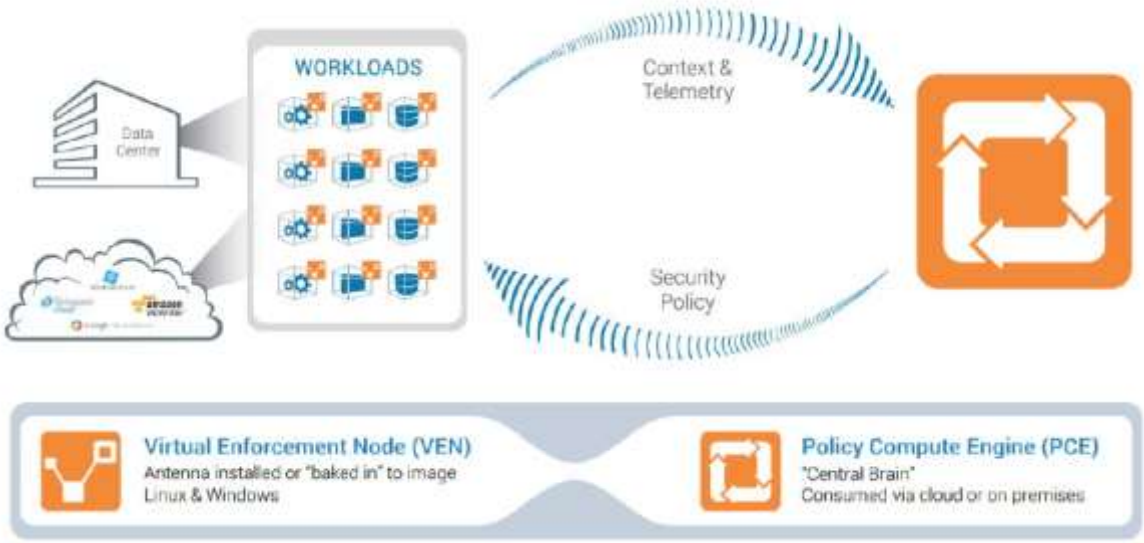

Figure 1: Illumio ASP Deployment

The TOE, Illumio Adaptive Security Platform (ASP), consists of the Policy Compute Engine (PCE) and the Virtual Enforcement Node (VEN). Together, these components form a distributed software platform that is designed to continuously protect communications within and, across, tiers of applications and hosts. The TOE enables administrators to create access control policies to secure and to implement granular segmentation of hosts and applications within enterprise network, effectively reducing the attack surface and securing the network.

Policy Compute Engine (PCE) allows administrators to control network access policies, manage users and domains, and perform other management functions. The PCE contextualizes all traffic flows, services, and processes on application Workloads to provide visibility and segmentation and offers policy-based control of communication among Workloads. Administrators access the PCE through a web browser-based user interface.

Virtual Enforcement Nodes (VEN) are installed on the host machines, or Workloads, that are part of the protected enterprise network. The VEN consumes policy defined by the PCE, and configures the Workload's Linux iptables or the Windows Firewall

Platform. The VEN also collects and reports information about the Workload to the PCE.

The ASP allows administrators to visualize application traffic and to implement continuous, scalable, and dynamic policy and enforcement to every Workload that represents bare-metal servers, VMs, containers, workstations, and VDIs within data centers, cloud, or distributed enterprise environments. A Workload is considered managed when VEN is installed and paired, or unmanaged when VEN is not present. The PCE is capable of defining policy that targets both managed and unmanaged Workloads, however policy can be enforced only by managed Workloads. The relationship between PCE and VEN is one to many.

3.1.1 PCE Node Types

The Policy Compute Engine (PCE) supports deployments in high-availability multi-node cluster configurations, but such a multi-node deployment is not evaluated. In the evaluated configuration PCE is deployed as a single node or 1 x 1 cluster, with both the Core and Data components residing on the same node.

3.2 *TOE Platform Requirements*

The TOE is a software application that relies on the hardware and features of an underlying operating system to operate.

3.2.1 Software Requirements

The TOE is designed to run on a host operating system that meets the following minimum requirements:

Table 3-1: PCE Supported Platforms

Component	Description
PCE	Red Hat Enterprise Linux 7.4

Table 3-2: PCE Software Dependencies

Component	Description

Component	Description
PCE	RHEL with the following packages: • coreutils • findutils • net-tools • procps • gawk • grep • util-linux-ng • sed • tar • bzip2
	RHEL with the following shared libraries: • glibc-2.12 • libgcc-4.4.7 • libstdc++-4.4.7 • ncurses-libs-5.7 • zlib-1.2.3

The VEN software is supported on the following host platforms, which in turn allows the PCE to manage these platforms:

Table 3-3: VEN Supported Platforms

Component	Description
VEN	Windows Server 2016
	Windows Server 2012 R2

3.2.2 Hardware Requirements

The PCE is capable of running on any hardware supported by RHEL 7.4. The size and complexity of managed network, measured in Workloads, determines recommended hardware requirements.

Table 3-4: Recommended Hardware Requirements

Max # of Workloads	Max # of Unmanaged Workloads	CPU Requirements	Memory Requirements	Drive Requirements
2,500	1,250	4 Core 2.4 GHz	32 GB	100 GB (Core) 250 GB (Data)
10,000	5,000	16 Core 3.2 GHz	128 GB	100 GB (Core) 250 GB (Data)

In the evaluated TOE configuration the VEN is installed on Windows Server 2012 R2 or Windows Server 2016. The VEN hardware requirements are defined by the host OS.

3.2.3 Other Requirements

DNS

All managed workloads must be able to consistently resolve the PCE's Fully Qualified Domain Name (FQDN). The FQDN must be resolvable on all managed Workloads, and for all users of the PCE Web UI.

X509 Certificates

An X.509v3 certificate must be installed on the PCE during its initial configuration. The certificate is uploaded as part of a certificate chain that contains the end-point or leaf certificate, and the chain of CA certificates (Intermediate and/or Root) needed to establish the chain of trust. When any client opens a TLS session to the PCE (e.g., pairing a Workload, accessing the PCE web console), the PCE will present its certificate to self-authenticate as part of establishing the communication.

The X.509v3 certificates used must meet the following basic criteria:

1. The file must contain PEM-encoded certificates.
2. The file must contain the leaf certificate and the entire certificate chain necessary to establish the chain of trust back to a trust anchor.
3. The leaf certificate identifier must match the PCE FQDN. This can be an exact match (e.g., pce.mycompany.com) or a wildcard match (e.g., *.mycompany.com).
4. The certificate must contain both TLS Web Server Authentication and TLS Web Client Authentication in the `extendedKeyUsage` field.
5. All CA certificate(s) in the chain must contain the `basicConstraints` extension with the `CA` flag set to `TRUE`.

3.2.4 Management Interface(s)

The TOE is managed via Web-based Management Interface (Web UI) implemented on PCE and compatible with any modern browser.

3.3 *TOE Boundary*

3.3.1 Physical Scope of the TOE

The TOE is a software application that is installed on the operating system running on the server hardware. The TOE does not include the hardware or the operating system on which it is installed. The PCE is delivered as an RPM package compatible with RHEL 7.4. The VEN this is an MSI compatible with Windows Installer 5.0 compatible with Windows Server 2016 or Windows Server 2012 R2. All installers are secured with end-user generated public key and downloaded from the vendor’s secure support portal.

3.3.2 Logical Scope of the TOE

The logical scope of the TOE is defined by the implemented security functionality (SF) as summarized in Section 1.4, TOE Security Functionality and further described in Section 7, TOE Summary Specification of this document.

The TOE relies on the host platform, Red Hat Enterprise Linux 7.4, to partially or fully implement the following SF:

- Cryptographic Support
- Protection of the TOE Security Function (TSF)
- Trusted Path/Channels

The software application that constitutes the TOE implements the following SF:

- Enterprise Security Management
- Security Audit
- Identification and Authentication
- Security Management
- TOE Access
- Trusted Path/Channels

3.3.3 TOE Architecture

The TOE is a distributed software application consisting of PCE that runs on Red Hat Enterprise Linux 7.4 and VEN that runs on Linux or Windows. Linux version of VEN is not evaluated.

The TOE relies on the following platform services:

- Cryptographic Modules (See Section 7.8 for details)
- Local Audit

The TOE implements the following TSFIs:

- Web UI (management interface)
- Audit Server Interface
- Domain Controller Interface
- NTP Interface
- VEN Control Interface

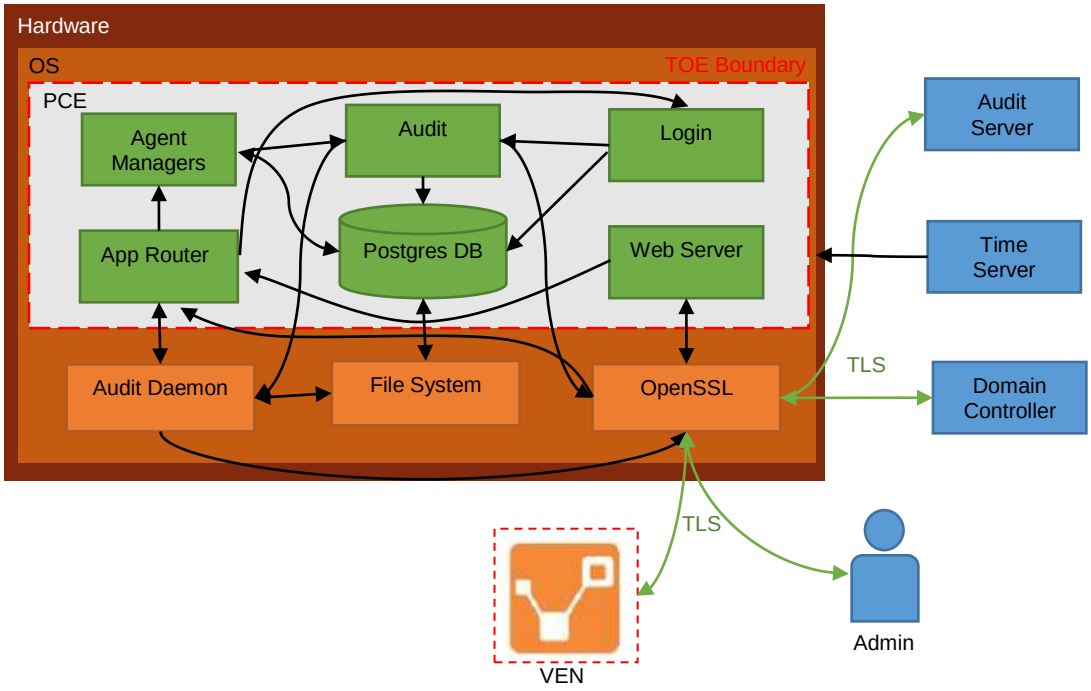

Figure 2: TOE Architecture

3.3.4 Operational Environment

- External management workstation
- Platform services:
  - Operating System (RHEL 7.4; Windows Server 2012 R2, Windows Server 2016)
    - Platform-provided Cryptographic Module (Red Hat Enterprise Linux OpenSSL Cryptographic Module, Windows Cryptographic Primitives Library)
  - Trusted Certificate Store
  - Syslog daemon (rsyslog or syslog-ng)
- External IT services:
  - Audit Server (syslog)
  - Authentication Server (SAML)
  - DNS Server
  - NTP Server
- Optional external servers
  - SMTP Server
  - External Certificate Authority (CA)

3.3.5 Excluded Functionality

The TOE supports a number of features that are not part of the core functionality. Those features are excluded from scope of the evaluation:

- Use of the SMTP is not evaluated
- High Availability and Failover functionality is not evaluated
- JSON/REST API use is not evaluated
- Policy-based encryption (SecureConnect) is not evaluated
- Configuration of policy targeting unmanaged Workloads is not evaluated
- Linux-based VEN is not evaluated

3.4 *TOE Guidance*

The following user guidance document is provided to customers and is considered part of the TOE:

Table 3-5: TOE Reference Documents

Reference Title	ID
Illumio Adaptive Security Platform 18.2.2 PCE Operations Guide 03/20/2019	[ADMIN]
Illumio Adaptive Security Platform 18.2.2 PCE Deployment Guide 03/20/2019	
Illumio Adaptive Security Platform 18.2.2 PCE Web Console User Guide Version 18.2.2	
Illumio Adaptive Security Platform 18.2.2 VEN Operations Guide 03/20/2019	
Illumio Adaptive Security Platform 18.2.2 VEN Deployment Guide 03/20/2019	
Illumio Adaptive Security Platform (ASP) Common Criteria Administrator Guide, Document Version 0.8, 03/06/2019	[CC Guide]

The documents in the following table were used as reference materials to develop this ST.

Table 3-6: ST Reference Documents

Reference Title	ID
Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1, October 24, 2013	[ESM PM PP]

4 Security Problem Definition

The Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1, October 24, 2013, [ESM PM PP], provides the following policies, threats and assumptions about the TOE.

4.1 *Threats*

This section identifies the threats applicable to the ESM PM PP, as specified in the Protection Profile, verbatim.

Table 4-1: TOE Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.CONDTRADICT	A careless administrator may create a policy that contains contradictory rules for access control enforcement.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FORGE	A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.UNAUTH	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
T.WEAKPOL	A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.

4.2 *Organizational Security Policies (OSPs)*

This section identifies the organizational security policies applicable to the ESM PM PP, as specified in the Protection Profile, verbatim.

Table 4-2: Organizational Security Policies

Policy Name	Policy Definition
P.BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

4.3 *Assumptions*

This section identifies assumptions applicable to the ESM PM PP, as specified in the Protection Profile, verbatim.

Table 4-3: Connectivity Assumptions

Assumption Name	Assumption Definition
A.CRYPTO	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.ROBUST	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
A.SYSTIME	The TOE will receive reliable time data from the Operational Environment.
A.USERID	The TOE will receive identity data from the Operational Environment.

Table 4-4: Personnel Assumptions

Assumption Name	Assumption Definition
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.

4.4 *Security Objectives*

This section defines the security objectives of the TOE and its supporting environment.

4.4.1 Security Objectives for the TOE

This section identifies Security Objectives for the TOE applicable ESM PM PP, verbatim.

Table 4-4: TOE Security Objectives

Objective	TOE Security Objective Definition
O.ACCESSID	The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH	The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.CONSISTENT	The TSF will provide a mechanism to identify and rectify contradictory policy data.
O.DISTRIB	The TOE will provide the ability to distribute policies to trusted IT products using secure channels.
O.INTEGRITY	The TOE will contain the ability to assert the integrity of policy data.
O.MANAGE	The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.
O.POLICY	The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control.
O.PROTCOMMS	The TOE will provide protected communication channels or administrators, other parts of a distributed TOE, and authorized IT entities.
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.

4.4.2 Security Objectives for the Operational Environment

This section identifies operational environment security objectives applicable to ESM PM PP, as specified in the Protection Profile, verbatim.

Table 4-5: Security Objectives for the Operational Environment

Objective	Environmental Security Objective Definition
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.
OE.CRYPTO	The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.PROTECT	One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.
OE.ROBUST	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.
OE.USERID	The Operational Environment shall be able to identify a user requesting access to the TOE.

5 Extended Components Definition

The components listed in the following table have been defined in the Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1, October 24, 2013, [ESM PM PP].

The extended components are denoted by adding "_EXT" in the component name. The extended class is denoted by "ESM_" in the component name.

5.1 *Extended Security Functional Components*

Table 5-1: Extended Components

Item	SFR ID	SFR Title
1	ESM_ACD.1	Access Control Policy Definition
2	ESM_ACT.1	Access Control Policy Transmission
3	ESM_ATD.1	Object Attribute Definition
4	ESM_EAU.2	Reliance on Enterprise Authentication
5	ESM_EID.2	Reliance on Enterprise Identification
6	FAU_SEL_EXT.1	External Selective Audit
7	FAU_STG_EXT.1	External Audit Trail Storage
8	FCS_HTTPS_EXT.1	HTTPS
9	FCS_TLS_EXT.1	TLS
10	FMT_MOF_EXT.1	External Management of Functions Behavior
11	FMT_MSA_EXT.5	Consistent Security Attributes
12	FPT_APW_EXT.1	Protection of Stored Credentials
13	FPT_SKP_EXT.1	Protection of Secret Key Parameters

5.2 *Extended Security Functional Components Rationale*

All extended security functional components are sourced directly from the ESM PM PP and applied verbatim.

6 Security Requirements

6.1 *Security Functional Requirements*

Conventions

The following conventions have been applied in this document:

- **Security Functional Requirements** – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - **Iteration**: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FDP_ACC.1 (a) and FDP_ACC.1 (b) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, “a” and “b”.
    - **Assignment**: allows the specification of an identified parameter. Assignments are indicated using bold italics and are surrounded by brackets (e.g., ***[assignment]).***
    - **Selection**: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., ***[selection]***).
    - **Refinement**: are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***italicized bold and underlined text***.

Note: Operations already performed in the ESM PM PP are not identified in this Security Target

The TOE Security Functional Requirements (SFRs) are listed in Table 6-1. All SFRs are based on requirements defined in Part 2 of the Common Criteria or defined in the ESM PM PP.

Table 6-1: TOE Security Functional Components

Functional Component		
1	ESM_ACD.1	Access Control Policy Definition
2	ESM_ACT.1	Access Control Policy Transmission
3	ESM_ATD.1	Object Attribute Definition
4	ESM_EAU.2	Reliance on Enterprise Authentication
5	ESM_EID.2	Reliance on Enterprise Identification
6	FAU_GEN.1	Audit Data Generation
7	FAU_SEL_EXT.1	External Selective Audit
8	FAU_STG_EXT.1	External Audit Trail Storage
9	FCS_HTTPS_EXT.1	HTTPS

Functional Component		
10	FCS_TLS_EXT.1	TLS
11	FIA_AFL.1	Authentication Failure Handling
12	FIA_SOS.1	Verification of Secrets
13	FIA_USB.1	User-Subject Binding
14	FMT_MOF.1	Management of Functions Behavior
15	FMT_MOF_EXT.1	External Management of Functions Behavior
16	FMT_MSA_EXT.5	Consistent Security Attributes
17	FMT_MTD.1	Management of TSF Data
18	FMT_SMF.1	Specification of Management Functions
19	FMT_SMR.1	Security Management Roles
20	FPT_APW_EXT.1	Protection of Stored Credentials
21	FPT_SKP_EXT.1	Protection of Secret Key Parameters
22	FTA_SSL.3	TSF-initiated Termination
23	FTA_SSL.4	User-initiated Termination
24	FTA_TAB.1	TOE Access Banner
25	FTP_ITC.1	Inter-TSF Trusted Channel
26	FTP_TRP.1	Trusted Path

6.1.1 Class ESM: Enterprise Security Management

6.1.1.1 ESM_ACD.1 Access Control Policy Definition

ESM_ACD.1.1 The TSF shall provide the ability to define access control policies for consumption by one or more compatible Access Control products.

ESM_ACD.1.2 Access control policies defined by the TSF shall be capable of containing the following:

Subjects: [***platform handler (workload)***] and

Objects: [***network traffic filter***]; and

Operations: [***create, update, delete***]; and

Attributes: [***inbound, outbound, src IP, dst IP, dst port, protocol***].

ESM_ACD.1.3 The TSF shall associate unique identifying information with each policy.

6.1.1.2 ESM_ACT.1 Access Control Policy Transmission

ESM_ACT.1.1 The TSF shall transmit policies to compatible and authorized Access

Control products under the following circumstances: [***at a periodic interval, after successful initial pairing***].

6.1.1.3 ESM_ATD.1 Object Attribute Definition

ESM_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual objects: [

Object: platform handler (workload)

Attributes: IP address, hostname, OS, pairing status

Object: network traffic

Attributes: source, destination, port, protocol

].

ESM_ATD.1.2 The TSF shall be able to associate security attributes with individual objects.

6.1.1.4 ESM_EAU.2 (1) Reliance on Enterprise Authentication (Password authentication)

ESM_EAU.2.1 (1) The TSF shall rely on [***PCE Login Service***] for subject authentication.

ESM_EAU.2.2 (1) The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

6.1.1.5 ESM_EID.2 (1) Reliance on Enterprise Identification (Username identification)

ESM_EID.2.1 (1) The TSF shall rely on [***PCE Login Service***] for subject identification.

ESM_EID.2.2 (1) The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

6.1.1.6 ESM_EAU.2 (2) Reliance on Enterprise Authentication (SAML authentication)

ESM_EAU.2.1 (2) The TSF shall rely on [***SAML Identity Provider***] for subject authentication.

ESM_EAU.2.2 (2) The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

6.1.1.7 ESM_EID.2 (2) Reliance on Enterprise Identification (SAML identification)

ESM_EID.2.1 (2) The TSF shall rely on [***SAML Identity Provider***] for subject identification.

ESM_EID.2.2 (2) The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

6.1.2 Class FAU: Security Audit

6.1.2.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions; and
b) All auditable events identified in Table 3 for the [not specified] level of audit; *and*
c) [***no other auditable events***].

Table 6-2: Auditable Events (ESM PM PP Table 3)

Component	Event	Additional Information
ESM_ACD.1	Creation or modification of policy	Unique policy identifier
ESM_ACT.1	Transmission of policy to Access Control products	Destination of policy
ESM_ATD.1	Definition of object attributes	Identification of the attribute defined
ESM_ATD.1	Association of attributes with objects	Identification of the object and the attribute
ESM_EAU.2	All use of the authentication mechanism	None
FAU_SEL_EXT.1	All modifications to audit configuration	None
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FCS_HTTPS_EXT.1	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FCS_TLS_EXT.1	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state	Action taken when threshold is reached
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret	None
FMT_SMF.1	Use of the management functions	Management function performed
FMT_SMR.1	Modifications to the members of the management roles	None
FTA_SSL.3	All session termination events	None
FTA_SSL.4	All session termination events	None
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel

Component	Event	Additional Information
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

FAU_GEN.1.2 The TSF shall record within each audit record 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; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***information specified in 'Additional Information' column of Table 6-2***].

6.1.2.2 FAU_SEL_EXT.1 External Selective Audit

FAU_SEL_EXT.1.1 The TSF shall be able to select the set of events to be audited by [an ESM Access Control product] from the set of all auditable events based on the following attributes:

a. [***event type***]; and

b. [***no other attributes***].

6.1.2.3 FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [***external syslog server, local Linux logs***].

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

6.1.3 Class FCS: Cryptographic Support

6.1.3.1 FCS_HTTPS_EXT.1 HTTPS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

6.1.3.2 FCS_TLS_EXT.1 TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

[

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

].

Note: This SFR modified to conform to TD0320.

6.1.4 Class FIA: Identification and Authentication

6.1.4.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [***5***] unsuccessful authentication attempts occur related to [***remote login attempts***].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [***lock the user account for 15 minutes***].

6.1.4.2 FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet the following:

a) For environmental password-based authentication, the following rules apply:
   1. Passwords shall be able to be composed of a subset of the following character sets: [***Standard ASCII character set***] that include the following values [***alphabet characters: a-z, A-Z, integers: 0-9, and a limited set of special characters:*** "!", "@", "#", "$", "%", "^", "&", "*", "?", ">","<"]; and
   2. Minimum password length shall settable by an administrator, and support passwords of 16 characters or greater; and
   3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and
   4. Passwords shall have a maximum lifetime, configurable by an administrator; and
   5. New passwords shall contain a minimum of an administrator-specified number of character changes from the previous password; and
   6. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based authentication, the following rules apply:
   1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

6.1.4.3 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [
Username
Email
Role
Scope
].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [***user security attributes are associated upon successful identification and authentication***].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [***changes to user security attributes take effect during the next action they make after the change***].

6.1.5 Class FMT: Security Management

6.1.5.1 FMT_MOF.1 Management of Functions Behavior

FMT_MOF.1 The TSF shall restrict the ability to [***determine the behavior of, disable, enable, modify the behavior of***] the functions: [***management functions identified in Table 6-3***] to [***management roles identified in Table 6-4***].

6.1.5.2 FMT_MOF_EXT.1 External Management of Functions Behavior

FMT_MOF_EXT.1.1 The TSF shall restrict the ability to query the behavior of, modify the functions of Access Control products: audited events, repository for audit storage, Access Control SFP, policy version being implemented, Access Control SFP behavior to enforce in the event of communications outage, [***pair Workloads***] to [***management roles identified in Table 6-4***].

6.1.5.3 FMT_MSA_EXT.5 Consistent Security Attributes

FMT_MSA_EXT.5.1 The TSF shall [***only permit definition of unambiguous policies***].

FMT_MSA_EXT.5.2 The TSF shall take the following action when an inconsistency is detected: [[***no action***]].

6.1.5.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [***delete***] the [***username, email***] to [***Global Organization Owner***].

6.1.5.5 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [***management functions listed in Table 6-3***].

Table 6-3: Management Functions within the TOE (ESM PP PM Table 4)

Requirement	Management Activities
ESM_ACD.1	Creation of policies
ESM_ACT.1	Transmission of policies
ESM_ATD.1	Definition of object attributes Association of attributes with objects
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
FAU_SEL_EXT.1	Configuration of auditable events for defined external entities
FAU_STG_EXT.1	Configuration of external audit storage location
FIA_AFL.1	Configuration of authentication failure threshold value Configuration of actions to take when threshold is reached Execution of restoration to normal state following threshold action (if applicable)
FIA_SOS.1	Management of the metric used to verify secrets
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes
FMT_MOF_EXT.1	Configuration of the behavior of other ESM products
FMT_MSA_EXT.5	Configuration of what policy inconsistencies the TSF shall identify and how the TSF shall respond if any inconsistencies are detected (if applicable)
FMT_MTD.1	Management of user authentication data
FMT_SMR.1	Management of the users that belong to a particular role
FTA_TAB.1	Maintenance of the banner
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)

6.1.5.6 FMT_SMR.1 Security Management Roles

FMT_SMR.1.1 The TSF shall maintain the roles [***user roles identified in Table 6-4***].

Table 6-4: User Roles and Permissions

Role	Permissions
Global	
Global Organization Owner	Perform all actions: add, edit, or delete any resource, organization setting, or user account
Global Administrator	Perform all actions except user management: add, edit, or delete any resource or organization setting
Global Read Only	View any resource or organization setting, but cannot perform any operations.

Role	Permissions
Global Policy Object Provisioner	Provision rules containing IP Lists, Services, and Label Groups, and manage Security Settings, but cannot provision Rulesets, Bound Services, or Virtual Servers, or add, modify, or delete existing policy items.
Global Ruleset Provisioner	Provision Rulesets within the All Applications, All Environments, and All Locations scope. They cannot add or modify any Rulesets.
Limited Scope	
Full Ruleset Manager	Add, edit, and delete all Rulesets within the specified scope Add, edit, and delete Rules when the Provider matches the specified scope The Rule Consumer can match any scope.
Limited Ruleset Manager	Add, edit, and delete all Rulesets within the specified scope Add, edit, and delete Rules when the Provider and Consumer match the specified scope Cannot manage Rules that use IP Lists, Custom iptables Rules, User Groups, Label Groups, iptables Rules as Consumers, or have Internet connectivity
Ruleset Provisioner	Provision Rulesets within specified scope

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6 Class FPT: Protection of the TSF

6.1.6.1 FPT_APW_EXT.1 Protection of Stored Credentials

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

6.1.6.2 FPT_SKP_EXT.1 Protection of Secret Key Parameters

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.1.7 Class FTA: TOE Access

6.1.7.1 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 *Refinement:* The TSF shall terminate a remote interactive session after an [*Authorized Administrator-configurable time interval of session inactivity*].

6.1.7.2 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 *Refinement:* The TSF shall allow *Administrator*-initiated termination of the *Administrator*'s own interactive session.

6.1.7.3 FTA_TAB.1 TOE Access Banner

FTA_TAB.1.1 *Refinement:* Before establishing a user session, the TSF shall display a *configurable* advisory warning message regarding unauthorized use of

the TOE.

6.1.8 Class FTP: Trusted Paths/Channels

6.1.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall be capable of using [***TLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: [***audit server, authentication server***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *transfer of policy data,* [[***transfer of authentication data, transfer of audit data***]].

Note: This SFR modified to conform to TD0245.

6.1.8.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall be capable of using *[**HTTPS**]* to provide a communication path between itself and remote users that is logically distinct from other communication channels and provides assured identifications of its end points and protection of the communicated data from modification, disclosure, and [[***substitution***]].

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *initial user authentication and execution of management functions*.

Note: This SFR modified to conform to TD0245.

6.2 *Security Assurance Requirements for the TOE*

6.2.1 TOE Security Assurance Requirements

This section defines the assurance requirements for the TOE. The assurance activities to be performed by the evaluator are defined in Sections 6 and Appendix C of the ESM PM PP. The ESM PM PP draws from the CC Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing. The TOE security assurance requirements, summarized in the table below, identify the management and evaluative activities required to address the threats identified in the ESM PM PP.

Table 6-5: Assurance Components

Assurance Class	Assurance Components	
Development	ADV_FSP.1	Basic Functional Specification
Guidance documents	AGD_OPE.1	Operational User guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability analysis

The following tables state the developer action elements, content and presentation elements and evaluator action elements for each of the assurance components.

Table 6-6: ADV_FSP.1 Basic Functional Specification

Developer action elements	
ADV_FSP.1.1D	The developer shall provide a functional specification.
ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
Content and presentation elements	
ADV_FSP.1.1C	The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.2C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
ADV_FSP.1.3C	The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.
ADV_FSP.1.4C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements	
ADV_ FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_ FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

Table 6-7: AGD_OPE.1 Operational User Guidance

Developer action elements	
AGD_OPE.1.1D	The developer shall provide operational user guidance.
Content and presentation elements	
AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.
AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
Evaluator action elements	
AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 6-8: AGD_PRE.1 Preparative Procedures

Developer action elements	
AGD_PRE.1.1D	The developer shall provide the TOE, including its preparative procedures.
Content and presentation elements	
AGD_ PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_ PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
Evaluator action elements	
AGD_ PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_ PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

Table 6-9: ALC_CMC.1 Labeling of the TOE

Developer action elements	
ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
Content and presentation elements	
ALC_CMC.1.1C	The TOE shall be labeled with its unique reference.
Evaluator action elements	
ALC_CMC.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 6-10: ALC_CMS.1 TOE CM Coverage

Developer action elements	
ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
Content and presentation elements	
ALC_CMS.1.1C	The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.
ALC_CMS.1.2C	The configuration list shall uniquely identify the configuration items.
Evaluator action elements	
ALC_CMS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 6-11: ATE_IND.1 Independent Testing – Conformance

Developer action elements	
ATE_IND.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
ATE_IND.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
ATE_IND.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

Table 6-12: AVA_VAN.1 Vulnerability Survey

Developer action elements	
AVA_VAN.1.1D	The developer shall provide the TOE for testing.
Content and presentation elements	
AVA_VAN.1.1C	The TOE shall be suitable for testing.
Evaluator action elements	
AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

7 TOE Summary Specification

This section describes the specific Security Functions of the TOE that meet the criteria of the security features that are described in Section 3.3.2 Logical Scope of the TOE.

This chapter describes the security functions:

- Enterprise Security Management (ESM)
- Security Audit (FAU)
- Cryptographic Support (FCS)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Protection of the TSF (FPT)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

7.1 *Enterprise Security Management (ESM)*

ESM_ACD.1

Policy Compute Engine

The Policy Compute Engine (PCE) computes and manages the security policies that are consumed by the Virtual Enforcement Node (VEN). The PCE examines the relationships between Workloads, computes the rules required to implement defined security policies, and distributes those rules to the VEN installed on each managed Workload.

Virtual Enforcement Node

The VEN is a software application installed on a managed system (any bare metal server or virtual machine with an operating system) that acts as an Access Control agent. Illumio's generic term for a monitored system is Workload.

The VEN has two main functions. First, it gathers detailed system and traffic information from the Workload and reports that information to the PCE. Second, it enforces a security policy defined by the PCE. When the VEN receives security policy updates from the PCE, it configures iptables on Linux and the Windows Filtering Platform (WFP) on Windows to enforce the security policy. VEN functionality is outside the scope of this evaluation.

The TOE's declarative policy model allows administrators to describe, in natural language, how applications are segmented from an operational perspective.

- Declarative model enforces the policy while abstracting the network complexity
- Natural-language security policies eliminate the need to know IP addresses, VLANs, subnets, zones, or security groups
- Whitelist model ensures the smallest attack surface by permitting only allowed connections vs. blocking long lists of unauthorized connections

The TOE's policy model supports a range of segmentation capabilities based on role (e.g., web server), application (e.g., HRM), environment (e.g., development), and location (e.g., Germany).

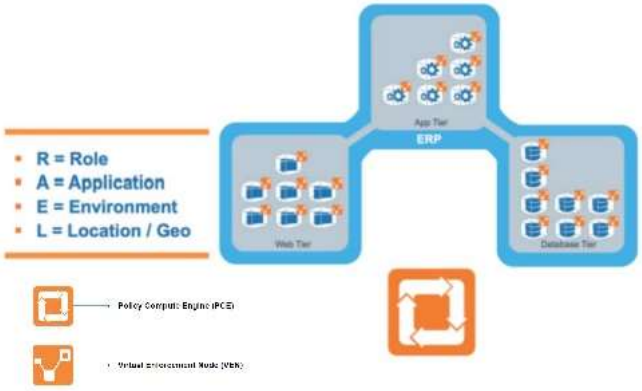

Figure 3: PCE Policy Model

The TOE uses labels to describe and match actions to objects. Labels are associated with a Workload during a pairing process. Label types include Role, Application, Environment, and Location. Each label identifies a specific category of Workloads, and those labels in rulesets are used to define the access control policy applicable to these Workloads.

Each policy consumed by VEN targets specific Workload, operates on a platform-specific traffic filter (e.g., Linux iptables), can create, update, or delete a traffic rule targeting inbound, outbound, source IP address, destination IP address, destination port, specific protocol.

ESM_ACT.1

The PCE generates policy that the VEN consumes and implements. When an administrator modifies or creates a natural-language security policy, the PCE generates an updated overall policy and calculates policy changes for each affected VEN as part of the process called provisioning. The policies generated by the PCE are identified with the `sec.policy.create` audit event. All paired VENs periodically connect to the PCE (by default, every 5 minutes) to check for policy updates. If the VEN cannot connect to the PCE, it continues to enforce the last-known-good policy. If the VEN fails to connect to PCE on two consecutive occasions (an outage approximately corresponding to 10 minutes), the VEN enters a degraded state.

There are two types of policy update modes – Adaptive Policy (the default setting) and Static Policy. In Adaptive Policy mode the PCE automatically accounts for moves, deployment scale, and changes to the applications and infrastructure that are typical of modern enterprise settings. When a change in policy occurs, the PCE responds dynamically by re-computing the firewall rules for the impacted Workloads. The PCE then calculates the update schedule and notifies all of the affected VENs that update is available. After receiving the notification, the VEN retrieves the updated rules and apply them immediately. When using Static Policy mode the Security Administrator schedules policy changes. In this mode, the TOE blocks the immediate application of new firewall rules that result from provisioning the policy changes and follows the specified periodic interval.

All policy updates are sent over an authenticated secure channel implemented with TLS. The VEN software is compatible with platforms specified in Table 3-3: VEN Supported Platforms.

ESM_ATD.1

The TOE uses labels to describe and match actions to objects. Labels are associated with a Workload during a pairing process. Workloads correspond to both specific platform and its network traffic. Each paired platform is tracked according to following attributes: IP address, hostname, OS, pairing status. When a paired platform generates network traffic, it has the following attributes: source, destination, port, protocol. The relationship between platform and its traffic is one to many. A policy can be defined based on these attributes to be a platform-wide (e.g., all traffic) down to micro-segmented (e.g., only UDP traffic on port 53 to 8.8.8.8).

ESM_EAU.2, ESM_EID.2

The TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. Users authenticate to the TOE by providing a username and password. TOE users authenticate either locally using direct login, or remotely via a configured domain controller (compatible with SAML) in the operational environment. When using a local login, user credentials are checked against the internal authorized users database. When using a domain login, the TOE initiates an authentication request to the external domain controller using supported protocols over a secure connection, and only allows user access after receiving a successful result message.

7.2 *Security Audit (FAU)*

FAU_GEN.1

The TOE is able to generate audit records of security relevant events as they occur. The events that result in an audit record are listed in Table 6-2. Generally, any use of a management functions via the Web UI, as well as relevant IT environment events, will be audited. The TOE uses the RHEL auditing daemon (`rsyslog` or `syslog-ng`) for storing local audit trail (e.g., in `/var/log/`), and is capable of uploading logs to an external audit server over a secure channel.

Local audit logs are stored as time-stamped records and include the event level, the date and time of the event, the source of the event, the event ID, task category, and where appropriate the outcome such as success or failure. Some audit records, such as errors, do not contain an explicit outcome statement. The local audit records can be viewed by authorized OS administrators using command line (e.g., tail -f) or compatible GUI utility (e.g., System Log Viewer).

FAU_SEL_EXT.1

The TOE collects audit events that are reported by managed Workloads (VEN). The authorized administrator can configure a severity level (INFO, WARNING, ERROR) for audit events collected from VENs.

FAU_STG_EXT.1

The TOE stores audit data locally, in the operational environment, by utilizing the Linux file system (e.g. `/var/log/`), and remotely by securely uploading audit records to an external audit server (e.g., syslog) in the operational environment. By default, all event logs are sent to

the local logs, and the TOE can be configured to duplicate that audit trail to a remote audit server. If remote logging is enabled, the TOE uses the syslog protocol (RFC 5424), encapsulated in the TLS protocol (RFC 5246), to secure the transmission of the audit data. No audit data is stored directly within the TOE boundary; the Operational Environment is expected to protect both the locally stored audit data and the audit data during transmission.

7.3 *Cryptographic Support (FCS)*

FCS_HTTPS_EXT.1

The TOE is managed via Web-based Management Interface (Web UI) accessible with any modern web browser. The TOE utilizes the Nginx 1.12 web server, configured for Strict Transport Security (RFC 6797) that enforces secure HTTPS (RFC 2818) connections. The web server implements the TLS v1.2 protocol and supports X.509v3 server authentication. A platform cryptographic module, Red Hat Enterprise Linux OpenSSL Cryptographic Module v5.0 implements all cryptographic functionality used by TLS protocol. OpenSSL is linked as a C library.

FCS_TLS_EXT.1

The PCE relies on platform's OpenSSL to implement TLS v1.2 (RFC 5246) with all claimed ciphers for the use with the external audit and authentication servers. The Red Hat Enterprise Linux OpenSSL Cryptographic Module v5.0 implements all cryptographic functionality used by the TLS protocol.

The VEN relies on platform's Cryptographic Primitives Library to implement TLS v1.2 (RFC 5246) with all claimed ciphers for communicating with PCE.

The following TLS ciphers are supported in the evaluated configuration:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

7.4 *Identification and Authentication (FIA)*

FIA_AFL.1

The TOE requires users to be identified and authenticated before they can access any of the TOE's functions. Users are locked out of their accounts when they fail to log in after 5 consecutive failures. Locked users retain all their privileges; however, they cannot log into the PCE for the duration of the lockout. When an account is locked, the web console reports that the username or password is invalid even when a user enters valid credentials. A user's locked account will reset after 15 minutes and therefore does not require an administrator to manually unlock it.

FIA_SOS.1

The TSF enforces the following rules for local administrator passwords:

- A password can contain standard ASCII alphabet characters (a-z, A-Z), integers (i.e., 0-9), and a limited set of special characters ("!", "@", "#", "$", "%", "^", "&", "*", "?", ">","<"). Blank spaces in passwords are not supported.
- Minimum password length is administrator configurable and passwords of 16 characters or greater are supported
- Administrator configurable password composition rules specifying required number of lower case, upper case, integers, and special character
- Administrator configurable password lifetime
- Administrator-specified character reuse from the previous password
- Administrator configurable password reuse history

The TOE also integrates with external authentication servers that manage external domain credentials. The TOE does not directly manages domain passwords and does not implement any SF that creates or modifies these credentials.

FIA_USB.1

The TOE associates all of a user's security attributes (e.g. username, email, role, scope) with the subjects acting on the behalf of that user. Users receive their privileges by way of membership in roles.

The TOE enforces the following rule on the initial association of a user's security attributes with subjects acting on the behalf of users: changes to user security attributes take effect during the next action that the user makes after the change has been made.

Each user's attributes are tracked against the session maintained by the TOE. Attribute changes for users are immediate and take effect during the user's next action. These attributes are constantly checked with every action a user takes during their session with the TOE.

7.5 *Security Management*

FMT_MOF.1

The TOE restricts management functions to authorized administrators. An administrator will authenticate to the TOE by providing their local or domain user credentials. If domain credentials are used, the TOE will interface with a remote authentication server. If the local credentials used, the local authentication identity store will be checked to determine if the credentials are valid. The TOE will next confirm that the user's account has not been locked or disabled, and will then allow the user access to the TSFs that are available to the user's defined role.

FMT_MOF_EXT.1

The TOE restricts management functions associated with the Access Control product (VEN) the same way that the TOE's own management functions are controlled. Only authorized administrators belonging to appropriate roles (see Table 6-4 for details) are capable of managing VENs. An administrator can pair, configure audit functionality, configure behavior to enforce in case of a communication outage, and configure the access control policy of VENs.

FMT_MSA_EXT.5

The TOE implements a whitelist access control policy model; consequently the TOE does not allow any contradictory policy to be defined.

FMT_MTD.1

The local authentication data repository is implemented as a table in the dedicated and integrated PostgreSQL database. Access to the data stored in this database is secured using the username/password authentication natively provided by the database as well as file permissions enforced by the operating system.

FMT_SMF.1

The TOE provides the management functions identified in Table 6-3.

FMT_SMR.1

The TOE maintains the roles defined in Table 6-4. Each authenticated user is automatically associated with a role. Global Organization Owners also have the ability to create custom roles and assign or change the scope of all Limited Scope roles.

7.6 *Protection of the security functionality*

FPT_APW_EXT.1

The TOE protects authentication data, such as stored passwords, so it is not directly accessible in plaintext. Locally stored password information is obscured by use of Bcrypt key stretching function. Additionally, when login-related configuration information is accessed through regular TOE interfaces, it is obfuscated by substituting the entered password characters with a series of asterisks.

FPT_SKP_EXT.1

X.509v3 certificates and their associated private keys are stored in the local file system protected by platform access control mechanism based on file permissions. All secrets, when stored in non-volatile memory, are encrypted by the platform when using an encrypting filesystem in the operational environment.

The operational environment implements all protocols and handles associated session keys. The TOE does not implement a mechanism designed to circumvent OS security measures.

7.7 *TOE access*

FTA_SSL.3

The TOE can be configured by an administrator to force an interactive session’s termination based on a timeout value (any positive integer value in minutes). A remote session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated. Once terminated, the user will be required to re-enter their user name and password in order to establish a new session.

FTA_SSL.4

Any administrative session can be terminated by logging out. Once terminated, the user will be required to re-enter their user name and password or re-authenticate with the domain controller to establish a new session.

FTA_TAB.1

The TOE, during initial installation, can be configured to display advisory banners as part of the authentication prompt.

7.8 *Trusted path/channels*

FTP_ITC.1, FTP_TRP.1

The TOE uses cryptographic primitives provided by the Operation Environment to implement secure channel functionality. ASP consists of two components PCE and VEN. PCE implements secure remote administration, exports audit records to an external audit server, integrates with an external authentication server, and securely transfers policy updates to VEN. VEN securely connects to PCE to receive policy updates.

The TOE can be configured to export audit records to an external audit server and synchronize with an external authentication server over a secure channel. In order to protect exported audit records and domain authentication data from disclosure or modification, the TOE implements the TLS v1.2 protocol. In both cases, the TOE acts as a client.

The TOE utilizes Nginx 1.12 web server to offer secure remote administration. The web server implements HTTP encapsulated in the TLS v1.2 protocol (i.e. HTTPS) and supports certificate-based server authentication. The TOE acts as a TLS server and presents X.509v3 certificate chain to connecting web clients.

The TOE supports SAML-based external authentication server (Active Directory Federation Services). The TOE acts as a SAML consumer and accepts digitally signed tokens as a proof of identity.

The TOE supports TLS v1.2 protocol to securely communicate between PCE and VEN. In this case, PCE acts as a server and VEN acts as a client.

PCE relies on platform (REHL 7) protocol library and cryptographic module. RHEL 7 is Common Criteria certified (Operating System Protection Profile evaluated at EAL 4) and implements the FIPS PUB 140-2 Level 1 (CMVP #3016) certified Red Hat Enterprise Linux OpenSSL Cryptographic Module that is also component validated for TLS key derivation function primitives (CVL 1338).

VEN (Windows) relies on platform protocol library and cryptographic module. Windows implements the FIPS PUB 140-2 Level 1 (see table below) certified Cryptographic Primitives Library.

OS	FIPS Certificate
Windows Server 2016 Cryptographic Primitives Library	CMVP #2937

Windows Server 2012 R2 Cryptographic Primitives Library	CMVP #2357

8 Security Problem Definition Rationale

This section identifies the mappings between the threats and objectives defined in the Security Problem Definition as well as the mappings between the assumptions and environmental objectives. In addition, rationale is provided based on the SFRs that are used to satisfy the listed objectives so that it can be seen that the mappings are appropriate.

Note: The Rationale text is from the ESM PM PP.

Table 8-1: Assumptions, Environmental Objectives, and Rationale

Assumptions	Objectives	Rationale
A.CRYPTO – The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.	OE.CRYPTO – The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	It is expected that vendors will typically rely on the usage of cryptographic primitives implemented in the Operational Environment to perform cryptographic protocols provided by the TOE.
A.ESM – The TOE will be able to establish connectivity to other ESM products in order to share security data.	OE.PROTECT – One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.	If the TOE does not provide policy data to at least one Access Control product, then there is no purpose to its deployment.
A.MANAGE – There will be one or more competent individuals assigned to install, configure, and operate the TOE.	OE.ADMIN – There will be one or more administrators of the Operational Environment that will be responsible for managing the TOE.	Assigning specific individuals to manage the TSF provides assurance that management activities are being carried out appropriately.
	OE.INSTALL – Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.	Assigning specific individuals to install the TOE provides assurance that it has been installed in a manner that is consistent with the evaluated configuration.
	OE.PERSON – Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.	Ensuring that administrative personnel have been vetted and trained helps reduce the risk that they will perform malicious or careless activity.
A.ROBUST– The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.	OE.ROBUST– The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	The ESM deployment as a whole is expected to provide a login frustration mechanism that reduces the risk of a brute force authentication attack being used successfully against the TSF and defines allowable conditions for authentication (e.g. day, time, location). It is expected that if the TSF does not provide this mechanism, then it will receive this capability from elsewhere in the ESM deployment.

Assumptions	Objectives	Rationale
A.SYSTIME – The TOE will receive reliable time data from the Operational Environment.	OE. SYSTIME – The Operational Environment will provide reliable time data to the TOE.	The TSF is expected to use reliable time data in the creation of its audit records. If the TOE is a software-based product, then it is expected that the TSF will receive this time data from a source within the Operational Environment such as a system clock or NTP server.
A.USERID – The TOE will receive identity data from the Operational Environment.	OE.USERID – The Operational Environment shall be able to identify a user requesting access to the TOE.	The expectation of an ESM product is that it is able to use organizationally-maintained identity data that resides in the Operational Environment.

Table 8-2: Policies, Threats, Objectives, and Rationale

Policies and Threats	Objectives	Rationale
P.BANNER – The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	O.BANNER – The TOE will display an advisory warning regarding use of the TOE.	FTA_TAB.1 The requirement for the TOE to display a banner is sufficient to ensure that this policy is implemented.
T.ADMIN_ERROR – An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	O.MANAGE – The TOE will provide Authentication Managers with the capability to manage the TSF.	FAU_SEL_EXT.1 FMT_MOF.1 FMT_MOF_EXT.1 FMT_MTD.1 FMT_SMF.1 By requiring authenticated users to have certain privileges in order to perform different management functions, the TSF can enforce separation of duties and limit the consequences of improper administrative behavior.
	OE.ADMIN – There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.	This objective requires the TOE to have designated administrators for the operation of the TOE. This provides some assurance that the TOE will be managed and configured consistently.
	OE.INSTALL – Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.	This objective reduces the threat of administrative error by ensuring that the TOE is installed in a manner that is consistent with the evaluated configuration.
	OE.PERSON – Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.	This objective reduces the threat of administrative error by ensuring that administrators have been properly vetted and trained prior to having access to the TOE.

Policies and Threats	Objectives	Rationale
T.CONTRADICT – A careless administrator may create a policy that contains contradictory rules for access control enforcement resulting in a security policy that does not have unambiguous enforcement rules.	O.CONSISTENT – The TSF will provide a mechanism to identify and rectify contradictory policy data.	FMT_MSA_EXT.5 The ability of the TSF to detect inconsistent data and to provide the ability to correct any detected inconsistencies will ensure that only consistent policies are transmitted to Access Control products for consumption.
T.EAVES – A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	OE.CRYPTO – The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	The TOE is able to establish and maintain trusted channels and paths by leveraging operational environment.
	O.DISTRIB – The TOE will provide the ability to distribute policies to trusted IT products using secure channels.	ESM_ACT.1 FTP_ITC.1 The TOE will leverage cryptographic tools to generate CSPs for usage within the product and its sensitive connections. The TOE will be expected to use appropriate CSPs for the encryption, hashing, and authentication of data sent over trusted channels to remote trusted IT entities.
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	FCS_HTTPS_EXT.1 FCS_TLS_EXT.1 FPT_SKP_EXT.1 FTP_ITC.1 FTP_TRP.1 Implementation of trusted channels and paths ensures that communications are protected from eavesdropping.
T.FORGE – A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.	O.ACCESSID – The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.	FTP_ITC.1 Requiring an Access Control product to provide proof of its identity prior to the establishment of a trusted channel from the TOE will reduce the risk that the TOE will disclose authentic policies to illegitimate sources. This reduces the risk of policies being examined for reconnaissance purposes.

Policies and Threats	Objectives	Rationale
	O.INTEGRITY – The TOE will contain the ability to assert the integrity of policy data.	FTP_ITC.1 Providing assurance of integrity of policy data sent to the Access Control product allows for assurance that the policy the Access Control product receives is the policy that was intended for it.
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	FCS_HTTPS_EXT.1 FCS_TLS_EXT.1 FPT_SKP_EXT.1 FTP_ITC.1 FTP_TRP.1 Implementation of a trusted channel between the TOE and an Access Control product ensures that the TOE will securely assert its identity when transmitting data over this channel.
	O.SELFID – The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.	FTP_ITC.1 Requiring the TOE to provide proof of its identity prior to the establishment of a trusted channel with an Access Control product will help mitigate the risk of the Access Control product consuming a forged policy.
	OE.CRYPTO **–** The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain trusted channels and paths when needed.
T.MASK – A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.	OE.SYSTIME – The TOE will receive reliable time data from the Operational Environment.	This objective helps ensure the accuracy of audit data by providing an accurate record of the timing and sequence of activities, which were performed against the TOE.

Policies and Threats	Objectives	Rationale
T.UNAUTH – A malicious user could bypass the TOE's identification, authentication, and authorization mechanisms in order to use the TOE's management functions.	O.AUTH – The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.	ESM_EAU.2 ESM_EID.2 FIA_USB.1 FMT_MOF.1 FMT_SMR.1 FPT_APW_EXT.1 FTP_TRP.1 The Policy Management product is required to have its own access control policy defined to allow authorized users and disallow unauthorized users specific management functionality within the product. Doing so requires the user to be successfully identified and authenticated and to have an established session such that the user is appropriately bound to their assigned role(s).
	O.MANAGE – The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.	FAU_SEL_EXT.1 FMT_MOF.1 FMT_MOF_EXT.1 FMT_MTD.1 (optional) FMT_SMF.1 The TOE provides the ability to manage both itself and authorized and compatible Access Control products. The management functions that are provided by the TSF are restricted to authorized administrators so they cannot be performed without appropriate authorization.
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	FCS_HTTPS_EXT.1 FCS_TLS_EXT.1 FPT_SKP_EXT.1 FTP_ITC.1 FTP_TRP.1 By implementing cryptographic protocols, the TOE is able to prevent the manipulation of data in transit that could lead to unauthorized administration.
	OE.CRYPTO – The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain a trusted path when needed.

Policies and Threats	Objectives	Rationale
T.WEAKIA - A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.	O.ROBUST - The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	FIA_AFL.1 FIA_SOS.1 FTA_SSL.3 FTA_SSL.4 If the TOE applies a strength of secrets policy to user passwords, it decreases the likelihood that an individual guess will successfully identify the password. If the TOE applies authentication failure handling, it decreases the number of individual guesses an attacker can make. If the TOE provides session denial functionality, it rejects login attempts made during unacceptable circumstances. If the TOE performs session locking and termination due to administrator inactivity, it decreases the likelihood that an unattended session is hijacked.
	OE.ROBUST – The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	This objective helps ensure that administrative access to the TOE is robust by externally defining strength of secrets, authentication failure, and session denial functionality that is enforced by the TSF.
T.WEAKPOL – A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.	O.POLICY – The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control.	ESM_ACD.1 ESM_ATD.1 FMT_MOF.1 FMT_SMF.1 The Policy Management product must provide the ability to define access control policies that can contain the same types of access restrictions that the Access Control products which consume the policy can enforce. These policies must be restrictive by default. This will ensure that strong policies are created that use the full set of access control functions of compatible products.

9 Acronyms and Terminology

9.1.1 CC Acronyms

The following table defines CC specific acronyms used within this Security Target.

Table 9-1: CC Acronyms from ESM PP PM

Acronym	Definition
CC	Common Criteria
CM	Configuration Management
CSP	Critical Security Parameter
DAC	Discretionary Access Control
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
OSP	Organizational Security Policy
PM	Policy Management
PP	Protection Profile
RBAC	Role-Based Access Control
RFC	Request for Comment
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

9.1.2 CC Terminology

The following table defines CC-specific terminology used within this Security Target.

Table 9-2: CC Terminology from the PP

Terminology	Definition
Access Control	A mechanism put in place to allow or deny the execution of defined operations requested by defined subjects to be performed against defined objects or the result achieved by employing such a mechanism.
Attribute-Based Access Control	A means of access control that is based upon the attributes of a user rather than the rights of a user. An example would be a system that grants access to specific resources if a user is an engineer and denies access to the same resources if the user is a contractor.
Authorized Administrator	A term synonymous with “Administrator”, used because some Common Criteria SFRs use the specific terminology.
Consume	The act of an Access Control product receiving a policy, parsing it, and storing it in a manner such that it can be used to enforce access control
Discretionary Access Control	A means of access control based on authorizations issued to a subject by virtue of their identity or group membership.
Enterprise Security Management	Systems and personnel required to order, create, disseminate, modify, suspend, and terminate security management controls
Identity and Credential Management Product	An ESM product that contains the primary functionality to store and manage identities and credentials within an ESM deployment for the purposes of identification and authentication.
Mandatory Access Control	A means of access control based on the notion that all subjects and objects within an enterprise are associated with one or more hierarchical labels. The dominance relationship assigned to these labels determines if access is permitted.
Operational Environment	The collection of hardware and software resources in an enterprise that are not within the TOE boundary. This may include but is not limited to third-party software components the TOE requires to operate, resources protected by the TOE, and the hardware upon which the TOE is installed.
Policy	A collection of rules that determine how the Access Control SFP is instantiated. These rules define the conditions under which defined subjects are allowed to perform defined operations against defined objects.
Policy Administrator	Within the context of the PP, this refers to one or more individuals who are responsible for using the TOE to generate and distribute policies.
Policy Enforcement Point	A component of an Enterprise Security Management that is responsible for applying the Access Control SFP to all relevant behavior in an enterprise. Synonymous with the Access Control product referred to within this PP.

Terminology	Definition
Policy Management product	An application that is responsible for creating policies that are consumed by the Policy Enforcement Point. These policies may be created through automated mechanisms, by manual administrative input, or by some combination of the two. This is the TOE as defined within this PP.
Role-Based Access Control	A means of access control that authorizes subject requests based on the roles to which they are assigned and the authorizations that are associated with those roles.
Secure Configuration Management Product	A product with the capability to alter the configuration of an ESM component and/or the ability to provision systems that reside in the Operational Environment
TOE Administrator	Within the context of the PP, this refers to the one or more individuals who are responsible for setting up the TOE, using the Policy Management product to define policies the TOE consumes, and reviewing audit data the TOE generates.
User	A blanket term for a generic user of the TOE; any entity that is identified and authenticated to the Policy Management product.

9.1.3 Product Acronyms and Terminology

The following table defines Product-specific acronyms and terminology used within this Security Target.

Table 9-3: Product-specific Acronyms and Terminology

Terminology	Definition
ASP	Adaptive Security Platform
FQDN	Fully Qualified Domain Name
PCE	Policy Compute Engine
VDI	Virtual Desktop Infrastructure
VEN	Virtual Enforcement Node
VM	Virtual Machine
Workload	A Workload represents a distinct collection of bare-metal servers, VMs, containers, workstations, and VDI within data centers, cloud, or distributed enterprise environments. A Workload is considered managed when VEN is installed, or unmanaged when VEN is not present