Illumio Core v24.2.20
Security Target

Version v0.5
June 6, 2025

Prepared By:

920 De Guigne Drive, Sunnyvale,
CA 94085

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 Core v24.2.20, which is a policy management product designed to manage access control policy within an enterprise environment.

1.1 Security Target Reference

ST Title: Illumio Core v24.2.20 Security Target

ST Version: v0.5

ST Author: Illumio

ST Date: June 6,2025

1.2 TOE Reference

TOE Developer: Illumio

Evaluation Sponsor: Illumio

TOE Identification: Illumio Core v24.2.20

Illumio Core [TOE] consists of two separate components:

- Policy Compute Engine (PCE)
- Virtual Enforcement Node (VEN).

The PCE will be version 24.2.20 and the VEN will be version 24.2.11.

Table 1-1: TOE Platforms

Series	Supported Platforms
Policy Compute Engine (PCE) v24.2.20	Red Hat Enterprise Linux 9.4 running on Intel Xeon Silver 4216
Virtual Enforcement Node (VEN) v24.2.11	Windows Sever 2022 running on Intel Xeon Gold 6130

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 2022, Revision 1, November 2022.

Assurance Level: Protection Profile Conformant

1.3 TOE Overview

1.3.1 TOE Product Type

The Target of Evaluation (TOE), Illumio Core v24.2.20, 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.

1.3.2 TOE Overview and Usage

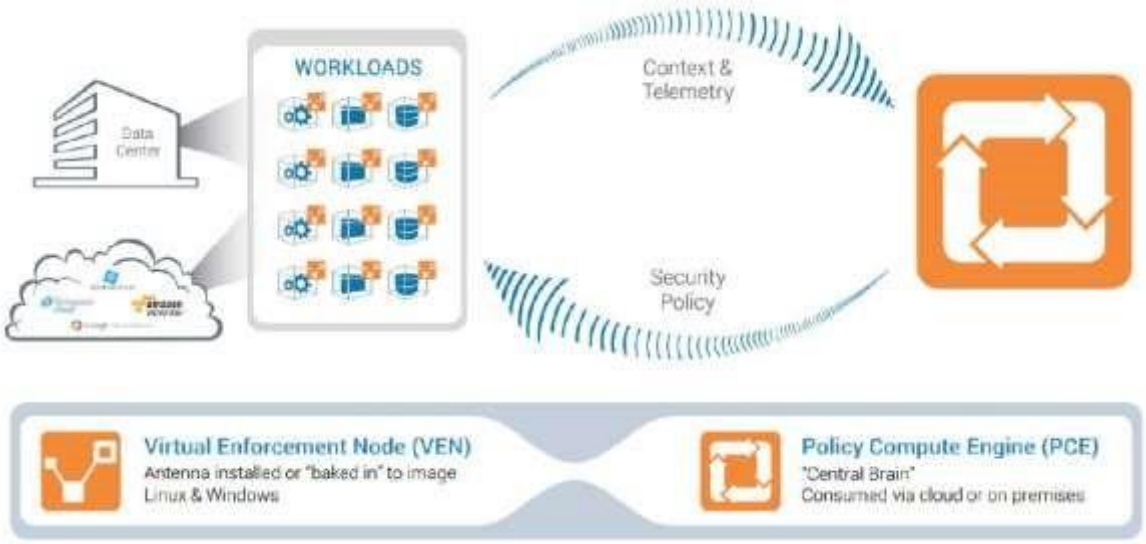

Figure 1: Illumio Core Deployment

The TOE, Illumio Core, 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 workload. Segmentation is another name for creating and sending (for enforcement) the firewall rules that separate traffic. A Workload represents a distinct collection of bare-metal servers, VMs, containers, workstations, and VDI within data centers, cloud, or distributed enterprise environments.

> ***Policy Compute Engine (PCE)*** allows administrators to control network access policies, manage users and domains, and perform other management functions. The Administrators access the PCE through a web browser-based user interface. The administrator has the ability to create policies and then provision them into the

VENs. Any rule that is not allowed by a policy will be disallowed by default when VENs are placed in enforcement mode.

[[Note: The scope of this evaluation is limited to policies, policy definition, and provisioning aspects offered by the PCE visualization feature. All other aspects of visualization are excluded]

Virtual Enforcement Nodes (VEN) are installed on the host machines, or Workloads, which are part of the protected enterprise network. The VEN has two main functions. a) gather detailed system and traffic information from the Workload and report that information to the PCE (not tested). B) enforce a security policy defined by the PCE (tested). The access control policies are defined in the PCE and then provisioned to the VEN. The VEN interprets the policies received from the PCE and prepares it for the host firewall. An example of a policy is to allow traffic from machines in the Asset Management app (source) to a web server of ERP App running on port 443 (destination). Once a policy is provisioned to a VEN, the VEN formulates it to a rule using host-based firewalls – the Windows Firewall on Windows. The policy then gets enforced by the native firewall. The host firewall is not part of the TOE. Only VEN is. The TOE uses an allow-list model, which means all traffic is blocked by default. Without a rule, traffic is not allowed to reach the hosts in an environment. The VEN also collects and reports audit events and other information about the Workload to the PCE.

The PCE allows administrators to visually display application traffic and to implement policies to every Workload. A Workload is considered managed when VEN is installed and paired (or unmanaged when VEN is not present). The PCE is capable of defining policies that targets managed (and unmanaged) Workloads, however policies can be enforced only by managed Workloads. The relationship between PCE and VEN is one to many.

1.3.2.1 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 1x1 cluster, with both the Core and Data components residing on the same node.

1.3.3 TOE Security Functionality

- Enterprise Security Management
- Security Audit
- Identification and Authentication

- Security Management
- Protection of the TOE Security Function (TSF)
- TOE Access
- Trusted Path/Channels

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 section “1.4.4 Logical Scope of the TOE” of this document.

1.3.4 Non-TOE Hardware/Software/Firmware

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

The Operational Environment of the TOE includes:

- External management workstation
  - Latest versions of Chrome, Mozilla Firefox or Microsoft Edge browser.
  - Compatible SSH client able to connect to RHEL 9.4 (if required for OS management
- Platform services:
  - Trusted Certificate Store
    - Installation specific; at minimum, store certificates in default /etc/pki/ca-trust directories (linked by /etc/ssl/certs/) using appropriate read-only permissions.
  - Syslog daemon (syslog-ng)
    - rsyslog 8.24.0 or higher, or syslog-ng 3.1.8 or higher.
  - Operating System (RHEL 9.4)
    - Platform-provided Cryptographic Module (Red Hat Enterprise Linux OpenSSL Cryptographic Module, Windows Cryptographic Primitives Library)
- External IT services:
  - Audit Server (syslog)
    - rsyslog 8.24.0 or higher, or syslog-ng 3.1.8 or higher.
  - Authentication Server (SAML)
    - Any SAML 2.0-compliant provider.
  - DNS Server
    - Any modern DNS bind service such as bind 9.16.
  - NTP Server
    - Any modern NTP or chronyd service such as chrony 4.5.
- Optional external servers

- SMTP Server
  - Any modern SMTP service such as postfix 3.5.
- External Certificate Authority (CA)
  - Installation specific; any modern CA implementation should be sufficient.

1.3.4.1 Software Requirements

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

Table 1-2: PCE Supported Platforms

Component	Description
PCE	Red Hat Enterprise Linux 9.4

Table 1-3: PCE Software Dependencies

Component	Description
PCE	RHEL with the following packages: • bash >= 4.0.0 • bzip2 • chkconfig • coreutils >= 8.4 • findutils >= 4.4.0 • gawk • glibc-langpack-en • grep • initscripts • logrotate >= 3.14.0 • net-tools >= 2.0 • procps >= 3.2.0 • sed • shadow-utils >= 4.1.0 • syslog-ng >= 3.23 or rsyslog • tar • util-linux >= 2.32
	RHEL with the following shared libraries: ▪ glibc-2.34 ▪ libgcc-11.3.1 ▪ libstdc++-11.3.1 ▪ ncurses-libs-6.2 ▪ libuuid-2.37.4 ▪ libxml2-2.9.13 ▪ openssl-libs-3.0.7 ▪ zlib-1.2.11

	▪ xz-libs-5.2.5 ▪ libxcrypt-4.4.18

For FIPS compliance, the following additional libraries are required:

- libcrypto
- libssl

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

Table 1-4: VEN Supported Platforms

Component	Description
VEN	Windows Server 2022

1.3.4.2 Hardware Requirements

The PCE is capable of running on any hardware platform supported by RHEL 9.4. The size and complexity of managed network, measured in Workloads, determines recommended hardware machine requirements.

Table 1-5: Recommended Hardware Requirements

Configuration	Max # of Workloads	Max # of Unmanaged Workloads	CPU Requirements	Memory Requirements	Drive Requirements
1 node (Single Node Cluster)	250	2500	3 cores @ 2.1 GHz	16 GB	50 GB
2x2 small (2 core nodes, 2 data nodes)	2,500	12,500	4 cores per node @ 2.1 GHz	32 GB	50 GB (Core) 250 GB (Data)
2x2 large (2 core nodes, 2 data nodes)	10,000	50,000	16 cores per node @ 2.1 GHz	128 GB	50 GB (Core) 1 TB (Data)
4x2 (4 core nodes, 2 data nodes)	25,000	125,000	16 cores per node @ 2.1 Ghz	128GB	50 GB (Core) 1 TB (Data)

The size and complexity of managed network, measured in Workloads, determines recommended hardware machine requirements.

1.3.4.3 Other Requirements

None.

1.3.4.4 Management Interface(s)

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

1.4 TOE Description

1.4.1 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 9.4. The VEN software is an MSI compatible with Windows Installer 5.0 compatible with Windows Server 2022. All installers are secured with end-user generated public key and downloaded from the vendor's secure support portal.

1.4.2 TOE Architecture

The TOE is a distributed software application consisting of PCE that runs on Red Hat Enterprise Linux 9.4 and VEN on windows operating system (see section 3.3.5 for excluded and untested platforms). The VEN is only evaluated on the Windows Server 2022 operating system.

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

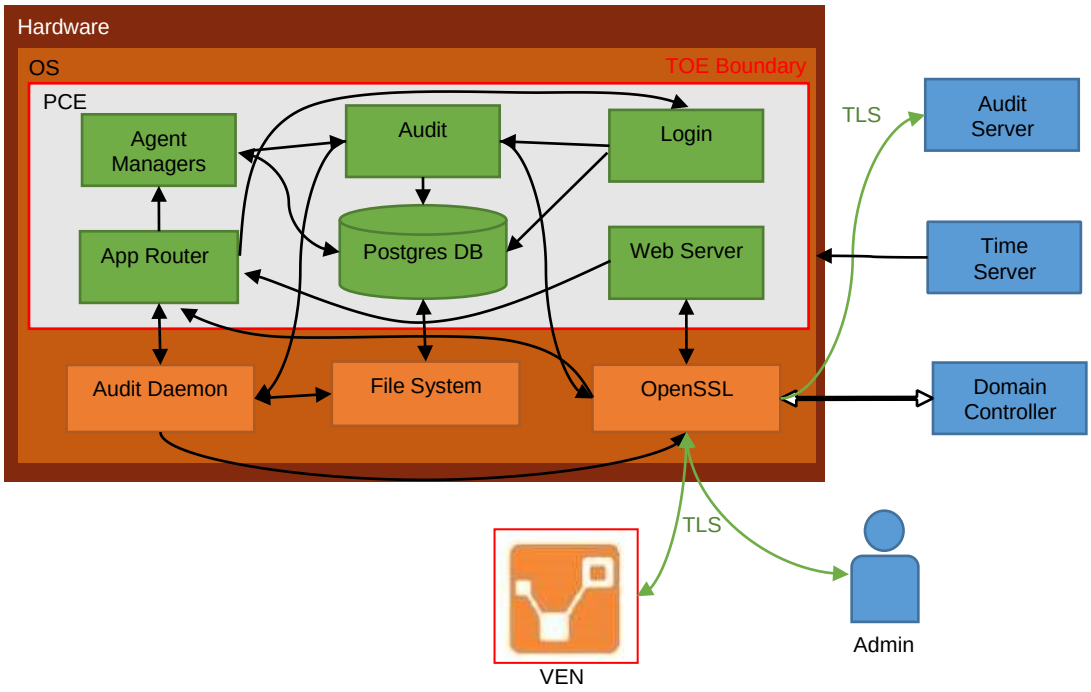

Figure 2: TOE Architecture

1.4.3 TOE Delivery

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

Table 1-6: TOE Reference Documents

Reference Title	ID	Format	Source/Download
Illumio Core Administration Guide 24.2.20 and 24.2.10	[ADMIN]	PDF	https://product-docs-repo.illumio.com/Tech-Docs/Core/PDFs/Illumio_Admin_Guide_24_2_20.pdf
Security Policy Guide 24.2.20 and 24.2.10		PDF	https://product-docs-repo.illumio.com/Tech-Docs/Core/PDFs/Security_Policy_Guide_24_2_20.pdf
Illumio Core 24.2.10 and 24.2.20 Install, Configure, Upgrade		PDF	https://product-docs-repo.illumio.com/Tech-Docs/Core/PDFs/Install_Config_Upgrade_24_2_20.pdf
Illumio Core Common Criteria Guide 24.2.20	[CC Guide]	PDF	https://product-docs-repo.illumio.com/Tech-

			Docs/Core/24.2/Common_Criteria/lllumio_Core_Common_Criteria_Guide_24.2.20.pdf

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

Table 1-7: ST Reference Documents

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

1.4.4 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.

1.4.4.1 Protection of the TOE Security Function (TSF)

The TOE protects sensitive data, such as stored passwords and secrets, so it is not directly accessible in plaintext.

1.4.4.2 Trusted Path/Channels

The TOE implements secure channels for communication for both the PCE and the VEN. PCE implements secure remote administration, exports audit records securely to an external audit server, integrates with an external authentication server, and securely transfers policy updates to VEN. The VEN securely connects to PCE to receive policy updates.

1.4.4.3 Enterprise Security Management

The TOE supports policy definition and transmission through its two primary components - PCE and VEN. The PCE computes and manages the security policies that are consumed by the VENs. The TOE allows administrators to define security policies and distributes those rules securely to the VENs which enforce those rules on the host using its native firewall.

1.4.4.4 Security Audit

The TOE allows audit of security related events and logging of such audit events securely to an audit server. The TOE is able to generate audit records of security-relevant events as they occur. Generally, any use of a management function via the Web UI, as well as relevant IT

environment events, will be audited. The agents (VENs) also send audit events to TOE by invoking the TOE's API
The TOE stores audit data locally, in the operational environment, by utilizing the Linux file system. The TOE is also capable of uploading audit records securely to an external audit server (e.g., syslog) in the operational environment.

1.4.4.5 Identification and Authentication

The TOE supports secure user authentication and handles authentication failures. The TOE requires users to be identified and authenticated before they can access any of the management functions. The TOE also enforces strong password policy and offers the ability to lockout users on unsuccessful user authentications.

1.4.4.6 Security Management

The TOE uses role-based access control to restrict access to management functions based on user's role. The TOE supports management capabilities listed in Table 6-3. The TOE restricts management functions associated with the VEN the same way that the TOE's own management functions are controlled. Only authorized administrators belonging to appropriate roles are capable of managing VENs.

1.4.4.7 TOE Access

The TOE can be configured by an administrator to force an interactive session's termination based on a timeout value. The TOE can also be configured to display advisory banners as part of the authentication prompt.

1.4.4.8 Trusted Path/Channels

The TOE implements secure channels for communication for both the PCE and the VEN. PCE implements secure remote administration, exports audit records securely to an external audit server, integrates with an external authentication server, and securely transfers policy updates to VEN. The VEN securely connects to PCE to receive policy updates.

1.4.5 Excluded Functionalities and platforms.

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

I. Use of the SMTP
II. High Availability and Failover functionality
III. JSON/REST API use
IV. Policy-based encryption (SecureConnect)
V. Configuration of policy targeting unmanaged Workloads
VI. Linux-based VEN
VII. LDAP Authentication

VIII. All visual aspects of the visualization feature, (also known as Illumination map), except the feature to add rules.

IX. Deny policies: only allow rules are evaluated.

X. Flexible label types: only the four default labels are evaluated (application, environment, location, role).

XI. Policy templates: the policies to be transmitted are generated from scratch.

XII. Windows outbound process-based enforcement: process-based enforcement allows more granular segmentation based on process name. The object “Windows outbound process” is not evaluated.

XIII. IPv6 support by the PCE and VEN

The TOE allows policies with multiple types of rules, destinations, and attributes. During the evaluation, a sample was taken to test most of them; the rest were not covered during the evaluation.

The following parameters were covered during the evaluation:

1. Subject attributes: IP address, hostname, OS and pairing status.
2. Labels: location, application, environment and role.
3. Policy operations: create, update and delete.
4. Rules:
    a. Traffic based on: inbound and outbound traffic.
    b. Destination and source based on: workload, IP, port.
    c. Protocols: ICMP, RDP, DNS.

The TOE runs on multiple platforms however, not all of them were tested, therefore they are not part of the evaluated configuration.

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 2022, Revision 1, November 2022, CCMB-2022-11-002*
    - Part 2 Extended

    Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 2022, Revision 1, November 2022, CCMB-2022-11-003

    - 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

- TD0844 - Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim
  - Addition of ALC_FLR.1
  - Applicable
- TD0794 - Correction to FCS_SSH_EXT.1.7 Test 2
  - Update the Test 2 of FCS_SSH.
  - Not applicable, ST does not claim FCS_SSH SFR.
- TD0621 – Corrections to FCS_TLS_EXT.1 in ESM PPs
  - Update of SFRs for TLS
  - Not applicable – OE provides all cryptography.
- TD0576 – FTP_ITC and FTP_TRP updated.
  - Reapplication of the FTP_ITC and FTP_TRP SFRs
  - Applied
- TD0574 – Update to FCS_SSH in ESM PPs
  - Update the FCS_SSH SFR to in line with current SSH standard.

  - Not applicable, ST does not claim FCS_SSH SFR.
- TD0573 – Update to FCS_COP and FCS_CKM in ESM PPs
  - Update the FCS_COP and FCS_CKM to in line with the current standard.
  - Not applicable – OE provides all the cryptographic operations.
- TD0079 – RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
  - Removal of ANS X9.31
  - Not applicable – OE provides all the cryptographic operations.
- TD0066 – Clarification of FAU_STG_EXT.1 Requirement in ESM PPs
  - External audit reconciliation clarified as optional.
  - Applied to FAU_STG.1
- 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 – OE provides all the cryptographic operations.

3 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.

3.1 Threats

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

Table 3-1: 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.

3.2 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 3-2: 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.

3.3 Assumptions

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

Table 3-3: 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 3-4: 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 Security Objectives

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

4.1.1 Security Objectives for the TOE

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

Table 4-1: 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.

4.1.2 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 4-2: 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	FMT_MOF_EXT.1	External Management of Functions Behavior
8	FMT_MSA_EXT.5	Consistent Security Attributes
9	FPT_APW_EXT.1	Protection of Stored Credentials
10	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 number in parenthesis placed at the end of the component. For example, FDP_ACC.1 (1) and FDP_ACC.1 (2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, "1" and "2".
- **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.1	Audit data storage location
9	FAU_STG.2	Protected audit data storage
10	FIA_AFL.1	Authentication Failure Handling
11	FIA_SOS.1	Verification of Secrets
12	FIA_USB.1	User-Subject Binding
13	FMT_MOF.1	Management of Functions Behavior
14	FMT_MOF_EXT.1	External Management of Functions Behavior

15	FMT_MSA_EXT.5	Consistent Security Attributes
16	FMT_MTD.1	Management of TSF Data
17	FMT_SMF.1	Specification of Management Functions
18	FMT_SMR.1	Security Management Roles
19	FPT_APW_EXT.1	Protection of Stored Credentials
20	FPT_SKP_EXT.1	Protection of Secret Key Parameters
21	FTA_SSL.3	TSF-initiated Termination
22	FTA_SSL.4	User-initiated Termination
23	FTA_TAB.1	TOE Access Banner
24	FTP_ITC.1	Inter-TSF Trusted Channel
25	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.1	Establishment and disestablishment of communications with audit server	Identification of audit server
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
FIA_SOS.1	Identification of any changes to the defined quality metrics	The change made to the quality metric
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
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available
FAU_GEN.1.1	Start-up and shutdown of the audit functions	Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event.

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. [***host identity***]; and
b. [**'Off', 'Blocked', or 'Allow +Blocked'**].

6.1.2.3 FAU_STG.1 Audit data storage location

FAU_STG.1.1 The TSF shall be able to store generated audit data on the [***transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC, local Linux logs***]

6.1.2.4 FAU_STG.2 Protected audit data storage

FAU_STG.2.1 The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG_2.2 The TSF shall be able to [***prevent***] unauthorized modifications to the stored audit data in the audit trail.

6.1.3 Class FIA: Identification and Authentication

6.1.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an administrator configurable positive integer within [**1 to 256**] 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*** **an administrator configurable positive integer within 1 to 256** ***number of minutes***].

6.1.3.2 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 be 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}.

6.1.3.3 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***].

6.1.4 Class FMT: Security Management

6.1.4.1 FMT_MOF.1 Management of Functions Behavior

FMT_MOF.1 The TSF shall restrict the ability to [**determine *the behavior of***] the functions: [***management functions identified in Table 6-3***] to [Global Organization Owner].

6.1.4.2 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***].

6.1.4.3 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***]].

6.1.4.4 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***].

6.1.4.5 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.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)

6.1.4.6 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 Viewer	View any resource or organization setting but cannot perform any operations.
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.
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 Viewer	View rules that match the scope. Cannot edit rulesets or rules.
Ruleset Provisioner	Provision Rulesets within specified scope
Workload manager	Manage workloads and pairing profiles within the specified scope. Read-only access provided to all other resources.
Ilo_pce	The ilo-pce user is a system account created when the PCE is installed. This is the only account used to operate the PCE, from starting/stopping to other PCE-related tasks such as backup and restore.

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

6.1.5 Class FPT: Protection of the TSF

6.1.5.1 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.

6.1.5.2 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.

6.1.6 Class FTA: TOE Access

6.1.6.1 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*].

6.1.6.2 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.

6.1.6.3 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.

6.1.7 Class FTP: Trusted Paths/Channels

6.1.7.1 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 TD0576.

6.1.7.2 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 TD0576.

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
	ALC_FLR.1	Basic Flaw Remediation
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: ALC_FLR.1 Basic Flaw Remediation

Developer action elements

ALC_FLR.1.1D	The developer shall document and provide flaw remediation procedures addressed to TOE developers.
Content and presentation elements	
ALC_FLR.1.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.1.2C	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.1.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.1.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
Evaluator action elements	
ALC_FLR.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Table 6-12: 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 6-13: 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 1.4.4 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)

7.1.1 TOE policy model

The Illumio PCE's policy model supports policies using either a label-based system or plain IP lists. By using labels, the rules don't require the use of an IP address or subnet as in traditional firewall solutions. Illumio PCE also supports the writing of IP list-based policies, like traditional firewalls.

To write label-based policy, workloads are first categorized using labels. The Illumio PCE supports four different types of labels: Application labels (ex: ERP, HCM, Asset-Management, etc.), Environment labels (ex: Production, Staging, Test, Dev), Location labels (ex: California, DC, Boston, etc.), and Role labels (ex: Database, Web, API, etc.).

Once workloads are labeled, administrators can write policies that use those labels. For example, an administrator can write a policy to allow traffic between the API Server of an ERP application to a specific port on the Database Server of the ERP application.

Here are some sample policies supported using the PCE policy model.

The API server of the ERP application is allowed to talk to the Postgres DB of the ERP application on port 5432.
Source: API (Role), ERP (Application) -> Destination: 5432 (Port) | Database (Role), ERP (Application)

The Web server of the ERP application is allowed to talk to the API server of the ERP server on port 8081.
Source: Web (Role), ERP (Application) -> Destination: 8081 (Port) | API (Role), ERP (Application)

All Corporate IPs specified in an IP list are allowed to talk to the Web server of ERP application on port 443.

Source: IP List (of Corporate IPs) -> Destination: 443 (Port) | Web (Role), ERP (Application)

These label-based policies are then converted into the appropriate rules for the OS-level firewalls of the workloads.

Policies can also be written using IP lists. So, for example:

Source: IP list (of some group of machines) -> Destination: 443 (port) | IP list of the VEN.

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 that acts as an Access Control agent. Illumio's generic term for a monitored system is Workload.

The VEN enforces a security policy defined by the PCE. When the VEN receives security policy updates from the PCE, it configures the ***Windows Filtering Platform*** (WFP) to enforce the security policy.

The TOE uses segmentation technology to create and enforce rules that separate traffic. This allows organizations to define and enforce policies down to the individual workload level. The PCE's declarative policy model allows administrators to describe, in constrained language, applications segmentation from an operational perspective.

- Declarative model enforces the policy while abstracting the network complexity.
- Constrained-language security policies eliminate the need-to-know IP addresses, VLANs, subnets, zones, or security groups
- Allow-list 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).

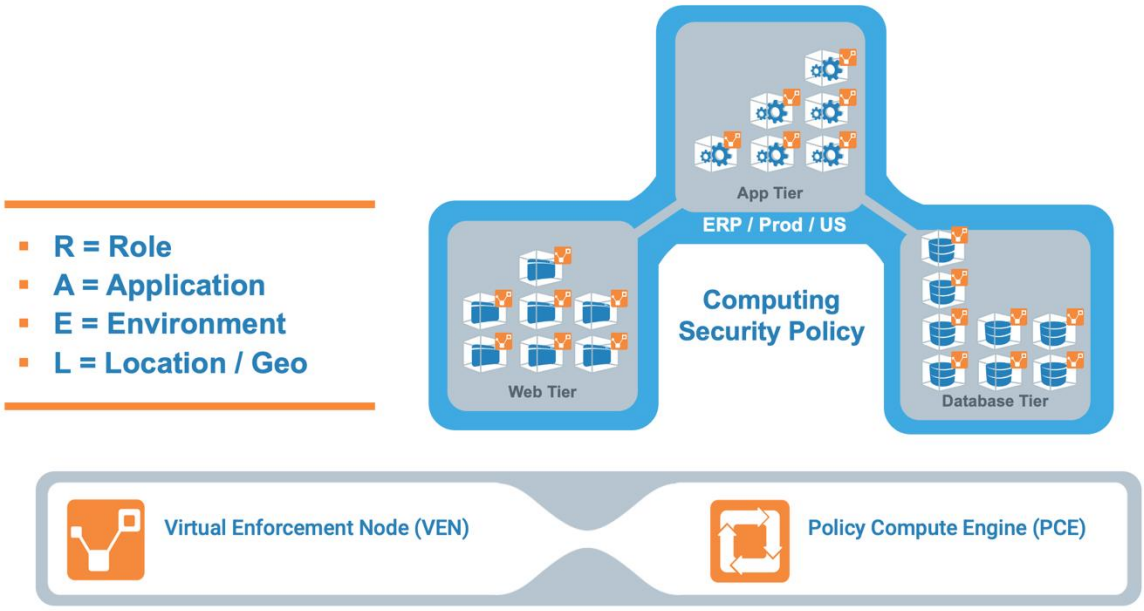

Figure 3: PCE Policy Model

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., Microsoft Firewall), 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 Constrained-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.

The PCE assigns a unique version number to each provisioned policy. Each time a policy is updated, the provisioned change gets a new version number. The PCE has one active version of the policy at one time. The older versions are considered historical versions. New policies provisioned to the VEN include a unique ID. With this ID, you can confirm the new policy version applied to the VEN is the same as the one currently provisioned on the PCE. To view

the policy generation on the VEN, enter the following command: ${persistent_data_root}/etc/firewall/debug/sec_policy.generation. There are two types of policy update modes – Adaptive Policy (the default setting) and Static Policy. In Adaptive Policy mode the PCE dynamically updates security policy when events, such as the following ones, occur in the managed environment.

- Workloads are added to or removed from your environment.
- Workloads change their IP addresses.
- Managed workloads come online and go offline.
- The labels on workloads change.

The PCE does not require Illumio users or automated processes to provision these changes for the PCE to re-compute the OS-level firewall rules for the impacted workloads. When the PCE re-computes rules, it 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 TLS secure channel. The VEN software is compatible with platforms specified in Table 3-3: VEN Supported Platforms.

The PCE administrator has also the option to create rules using the Illumination map feature, also called visualization map.. The feature of adding rules using the illumination map was evaluated and included in the TOE boundary, other features of the illumination map were not evaluated.

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 a 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 user 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, such as startup/ shutdown of the TOE software, will be audited. The PCE 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.

VEN does not use the Windows audit daemon. The VEN sends the following types of audit events to the PCE by invoking the PCE API

- Heartbeat events are reported every 5 minutes.
- Traffic flows are reported every 10 mins. The VEN reports traffic flow logs to PCE every 10 mins. The PCE logs these as audit events. Traffic flows that are created and deleted within the 10 min interval are also reported by the VEN to the PCE at the completion of the 10 min interval.
- Changes to network interfaces are reported asynchronously.

The PCE generates audit events when the APIs are invoked.

Local audit logs are stored in the local Linux filesystem as time-stamped records and include the event level (Informational, Warning, Error), the date and time of the event, subject identity, the source of the event, the event ID, task category, the outcome such as success or failure and where appropriate other information. Additionally, specific audit events will include other data based on the ‘Additional Information’ columns in Table 6-2. The local audit records can be viewed by authorized TOE’s administrators using the PCE management interface.

FAU_SEL_EXT.1

The VEN is capable of recording audit events for the connections of the workloads in which they are deployed.

The PCE displays audit events that are reported by managed Workloads (VEN) selected on VEN host-id and an additional selectable audit attribute: ‘Off’, ‘Blocked’ or ‘Allowed+Blocked’.

The VEN inspects all open ports on a workload and reports the flow of traffic between it and other workloads to the PCE. In this state, the PCE displays the flow of traffic to and from the workload, providing insight into the datacenter and the applications running in it. No traffic is blocked in this state. This state is useful when firewall policies are not yet known. This state can be used for discovering the application.

You can choose one of three modes for the traffic visibility for workloads:

Off (no detail): The VEN does not collect any details about traffic connections. This option provides no Illumination detail and utilizes the least amount of resources from workloads. This state is useful when you are satisfied with the rules that have been created and do not need additional overhead from observing workload communication.

Blocked: The VEN only collects the blocked connection details (source IP, destination IP, protocol and source port and destination port), including all packets that were dropped. This option provides less Illumination detail but also demands fewer system resources from a workload than high detail.

Blocked + Allowed: The VEN collects connection details (source IP, destination IP, protocol and source port and destination port). This applies to both allowed and blocked connections. This option provides rich Illumination detail but requires some system resources from a workload.

FAU_STG.1 & FAU_STG.2

The PCE component of the TOE stores audit data locally, in the OS 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 events are logged in the local logs. PCE can be configured to transfer the audit trail to a remote audit server. For remote logging, 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. The audit data cannot be deleted through the Web UI.

The PCE does not do audit log reconciliation when the connection to the syslog server is lost. If the connection between the audit server and the PCE is broken, there may be a gap in the audit server audit record. If log messages cannot be forwarded to their destination for some reason, the PCE keeps them in the queue and monitors the length of the queue. The status of syslog message forwarding is displayed in the health page of the Web Console. The possible status messages are Normal (fewer than 5,000 messages in queue), Long message queues (5,000 or more messages in queue), or Dropping messages. When PCE health becomes critical due to loss of the syslog forwarding connection, a message is logged in system_health.log. If a syslog connection is broken, an attempt is made to reconnect to the external syslog destination every 60 seconds.

7.3 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 consecutive failures. The number of unsuccessful authentication attempts can be configured by changing the default value of the runtime variable max_failed_login_attempts in the configuration file (default: 5; minimum: 1; maximum: 256). Similarly, the lockdown period can be configured by changing the default value of account_lockout_duration_minutes (default: 15; minimum: 1; maximum: 256). 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 a configurable time parameter and therefore does not require an administrator to manually unlock it.

The PCE enforces unsuccessful authentication thresholds only for local users. For users who log in through a SAML SSO Provider (IdP), the PCE does not store passwords and relies on the SAML Identity Provider to enforce a configurable unsuccessful authentication threshold. Actions on exceeding unsuccessful authentication thresholds must be configured at the SAML IdP.

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 between 8 and 64 characters, default length is 8, In the Common Criteria evaluated configuration the administrator is required to set the minimum length to 16.
- Administrator configurable password composition rules specifying required number of lower cases, upper cases, 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 manage 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 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.

7.4 Security Management

FMT_MOF.1

The TOE has the ability to determine the behavior of functions listed in Table 6-3 and restricts them to the “Global Organization Owner” administrator role. 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 are 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 an allow-list access control policy model. In an allow-list policy control model, all traffic flows are denied by default, unless an explicit rule is defined to allow a specific flow. This implies a flow is only possible when a rule is in place to enable it.

For example, if you have two workloads that compose a simple application – a web server and a database server – to allow these two workloads to communicate, a rule must be written that allows the required traffic between the workloads. Before any rules are written, all traffic between the workloads is denied by default. As you add rules, each rule allows some subset of traffic to occur. The effects of rules can only be additive: more traffic is allowed by each rule. Traffic allowed by one rule cannot negate or conflict with the traffic allowed by another rule. Consequently, the TOE does not allow 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.

The PCE stores the database password in an encrypted file. The key used to encrypt the file is generated using OpenSSL library running in FIPS mode on a CC evaluated OS. The key material is stored in a separate protected file on the TOE. This file and its containing folder are only accessible to the TOE's administrator on the machine.

The VEN stores secrets in an encrypted file. It uses the Windows DP (Data Protection) API to encrypt and store secrets.

Both the PCE and the VEN secrets are accessible only to root/administrator users.

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 have the ability to assign roles to users.

The ilo-pce user (also called PCE runtime user) is a system account created when the PCE is installed. This is the only account used to operate the PCE, from starting/stopping to other PCE-related tasks such as backup and restore. This account cannot be used to login to the Linux OS as it is a system account. This account cannot control or install security policies in VENs. This account cannot access the PCE WebUI and has no direct access to the database. The ilo-pce is the only system account used by the PCE and no other user accounts are used. The PCE and its services run under this account.

7.5 Protection of the security functionality

FPT_APW_EXT.1

The Illumio Product internally uses the database as a persistent store to ensure its proper functioning. Login credentials to the PCE console, i.e., passwords of users who are authorized to access the Product, are also stored in the database. Users' password credentials are stored in the form of salted hashes in the database. The database itself is internal to the Illumio Product.

The PCE protects authentication data, such as stored passwords, so it is not directly accessible in plaintext. Additionally, when login-related configuration information is accessed through regular TOE interfaces, the password is displayed 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.

The username and password used to access the database is protected as follows:

- ✓ The database username and password are stored encrypted using AES256-CBC in a protected file on the PCE machine.
  - This file and its containing folder are only accessible to the PCE administrator on the machine.
  - The password itself is 32-bytes (32-bytes full binary and then base64 encoded) automatically generated by OpenSSL running in FIPS mode on the CC evaluated RHEL 9.4 OS.
- ✓ The key material for the encryption key and IV used to encrypt the database password is generated by OpenSSL running in FIPS mode. The key material is stored in a separate protected file on the PCE.
  - This file and its containing folder are only accessible to the PCE administrator on the machine.

All secrets, when stored in non-volatile memory, are encrypted by the platform through the use of an encrypting filesystem in the operational environment. This usage is in accordance with configuration of the operational environment as per the AGD.

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

7.6 TOE access

FTA_SSL.3

The PCE component of 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 issued from the remote client) for the defined timeout value will be terminated. Once terminated, the user will be required to re-enter their username 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 username 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.

7.7 Trusted path/channels

FTP_ITC.1, FTP_TRP.1

The PCE and VEN uses cryptographic primitives provided by the Operation Environment to implement secure channel functionality. Illumio Core 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 PCE component of the TOE can be configured to export audit records to an external audit server over a secure channel. In order to protect exported audit records and domain authentication data from disclosure or modification, the TOE uses the 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.

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

The TOE uses 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 (RHEL 9.4) protocol library and cryptographic module. The RHEL 9.4 implements the FIPS PUB 140-3 Level 1 (CMVP # 4857) certified Red Hat Enterprise Linux OpenSSL FIPS provider which is also component validated for TLS key derivation function primitives.

VEN (Windows) relies on Microsoft Windows Server 2022 platform protocol library and cryptographic module to carry all its cryptographic operations. Microsoft Windows Server 2022 operating system is Common Criteria certified TOE (by NIAP scheme) conforming to the General-purpose operating system v4.2.1 protection profile and listed in the NIAP PCL under the name “Microsoft Windows 11 (version 22H2), Microsoft Windows 10 (version 22H2), Microsoft Windows Server 2022, Microsoft Windows Server Datacenter: Azure Edition, Microsoft Azure Stack HCIv2 version 22H2, Microsoft Azure Stack Hub, Microsoft Azure Stack Edge”.

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 reduces 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.

Policies and Threats	Objectives	Rationale
	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.
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.	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.	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 mitigates 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 ensures the accuracy of audit data by providing an accurate record of the timing and sequence of activities, which were performed against the TOE.
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

Policies and Threats	Objectives	Rationale
		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.	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.
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

Policies and Threats	Objectives	Rationale
		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 ensures 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
Illumio Core components	The relationship and basic architecture of the platform's components—the Policy Compute Engine (PCE) and the Virtual Enforcement Node (VEN). Understanding the inter-action between the PCE and VEN is essential to learning about Illumio technology.
Policy Compute Engine (PCE)	The brain of the Illumio Core. The Illumio Core stores its program logic and the information it collects in the PCE. The PCE generates and distributes segmentation policies for each VEN connected to it.
VDI	Virtual desktop infrastructure (VDI) is the hosting of desktop environments on a central server. It is a form of desktop virtualization, as the specific desktop images run within virtual machines (VMs) and are delivered to end clients over a network. Those endpoints may be PCs or other devices, like tablets or thin client terminals.
Virtual Enforcement Node (VEN)	The local control point of the Illumio Core installed on each workload. It provides information about the workload and enforces policy rules by controlling the Linux iptables or Windows Filtering Platform (WFP) tables on a workload.
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
Workload Policy States	The VEN supports multiple policy states to aid with the policy creation process. Illumination shows these states and uses them to visualize traffic.
Pairing	The process of installing the Illumio VEN software on a workload by using a unique secure pairing key.
Rulesets and Rules	The allow-list policies that use labels to generate customized port connections for each workload. Rules are collected into rulesets for versioning. Policies are pushed out to workloads with the matching labels by a process called provisioning.
Providers and Consumers	The Illumio model is provider centric. The Administrator declares the ports on providers that can be accessed by consumers.

Micro-segmentation	A security technique that enables fine-grained security policies to be assigned to applications, down to the workload level. It is built around two key principles: granularity and dynamic adaptation. The application of these principles makes micro-seg-mentation fundamentally different from conventional network segmentation.
Constraint Language or Constraint programming	is a paradigm for solving combinatorial problems that draws on a wide range of techniques from artificial intelligence, computer science, and operations research.