Assurance Activity Report
For
Illumio Core v22.2.30

Version v0.7

March 01,2023

Produced by:

DEKRA

DEKRA Cybersecurity Certification Laboratory Inc.
405 Glenn Dr, Suite 12, Sterling, VA 20164

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:

Illumio Inc.

920 De Guigne Drive, Sunnyvale, CA 94085

The Security Target was developed by:

Illumio Inc.

920 De Guigne Drive, Sunnyvale, CA 94085

The TOE Evaluation was sponsored by:

Illumio Inc.

920 De Guigne Drive, Sunnyvale, CA 94085

Contents

1. Introduction

This document summarizes the evaluation results of the Target of Evaluation (TOE), Illumio Core Platform v22.2.30 conforming to Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1, October 24, 2013, by listing the assurance activities and associated results as performed by the evaluators.

1.1 References

The following table provides information needed to identify and to control the Security Target (ST), the Target of Evaluation (TOE), and other evidence used in this evaluation.

Item	Identifier	Short Form
Security Target	Illumio Core V22.2.30 Security Target 0.6, March 1, 2023	[ST]
Protection Profile	Standard Protection Profile for Enterprise Security Management Policy Management, Version 2.1, October 24, 2013.	[PP]
User Guidance	Illumio Core v22.2.30 Common Criteria Guide, February 2023	[CC GUIDE]
	Illumio_Core_PCE_Administration_Guide_22.2	[PCE GUIDE]
	Illumio_Core_Security_Policy_Guide_22.2.1	[SP GUIDE]
	Illumio_Core_VEN_Administration_Guide_22.2.0	[VEN GUIDE]
Test Report	Illumio core v22.2.30 Evaluator Test Report version 0.6 March 1, 2023	[TR]

Table 1: Guidance and Reference Documents

1.2 Target of Evaluation

The TOE, Illumio Core Platform (ASP) v22.2.30, is an enterprise policy management product. The TOE's primary purpose is to manage communications within, and across, tiers of applications by defining access control policy. The TOE is a distributed software application that consists of the Policy Compute Engine (PCE) and the Virtual Enforcement Node (VEN). The VEN is an Access Control product which consumes and enforces policies created by the PCE. Together, these components form a distributed software platform designed to continuously protect communications within and, across, tiers of applications and hosts. The PCE enables administrators to create access control policies to secure and to implement granular segmentation of hosts and applications within enterprise network, effectively reducing the attack surface and securing the network. In the evaluated configuration the PCE is a software application running on Red Hat Enterprise Linux 8.2 with FIPS mode enabled and deployed as a Single Node Cluster (SNC) with both the Core and Data components residing on the same node. Virtualization, clustering, and high-availability configurations were not evaluated.

1.2.1 TOE Platform Requirements

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

1.2.1.1 Software Requirements

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

Table 2: PCE Supported Platforms

Component	Description
PCE	Red Hat Enterprise Linux 8.2

Table 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 • 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 • zlib >= 1.2.11

	RHEL with the following shared libraries: ▪ glibc-2.28 ▪ libgcc-8.3.1 ▪ libstdc++-8.3.1 ▪ ncurses-libs-6.1 ▪ libuuid-2.32 ▪ libssl.so., libcrypto.so. (openssl >= 1.1.1) ▪ libreadline.so. (readline >= 7.0) ▪ libselinux.so.1 (libselinux >= 2.9)

For FIPS compliance, the following additional libraries are required:

- libcrypto
- libssl

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

Table 4: VEN Supported Platform

Component	Description
VEN	Windows 10 Enterprise

1.2.1.2 TOE Equivalence

The following platforms were provided by the vendor for testing PCE:

Table 5: Evaluated Platforms

Component	Hardware Description	Operating system
PCE	Dell EMC PowerEdge R630 powered by an Intel Xeon Silver 4216 CPU	Red Hat Enterprise Linux 8.2
VEN	Dell Precision 3540 powered by an Intel Core i7-8665U CPU	Windows 10 Enterprise

Rationale for selection of platform for testing

The PCE is a software application that runs on top of a host machine's operating system. The vendor specified the minimum software and hardware requirements in the ST Section 3.2.2 Table 3-4, which matches the provided hardware above. The vendor-provided platform for testing the PCE component of the TOE, a Dell PowerEdge R630 runs on Intel Xeon Silver 4216, which matches one of the CPUs listed for the CMVP listing of RHEL 8.2.

The VEN is a software application that runs on top of a host machine's operating system. The vendor specified the minimum software and hardware requirements in the ST Section 3.2.2 Table 3-4, which matches the provided hardware in Table 2-4 above. The vendor-provided platform for testing the VEN component of the TOE, a Dell Precision 3540 powered by an Intel Core i7-8665U, which matches one of the CPUs listed for the CMVP listing of Windows 10 Enterprise Edition.

This setup, meeting the specified requirements, covers the claimed OSes for the PCE and VEN components of the TOE, and the VEN and the PCE match one of the platforms claimed in the ST Section 3.2.2 Table 3-4. Therefore, this setup is both representative and suitable for testing the TOE.

The TOE consists of two elements (PCE and VEN), both at software version 22.2.30 which were fully tested. As a result of full coverage, the requirement to present equivalency argument is trivially satisfied.

1.3 Testing Topology

The topology is configured for a dedicated 'Test' LAN for CC testing. This LAN is physically isolated via a dedicated core switch, preventing general access while still granting testers direct access to the TOE. The setup consists of a 'Test' LAN – 192.168.0.x for IPv4. The server is local to the 'Test' LAN and packet capture was done by a VMware Virtual machine, in a ESXi server, connected to a mirrored port on the switch.

During the testing assurance activity, the evaluator setup the PCE running version 22.2.30 running on a Linux RedHat enterprise version 8.2, also a VEN version 22.2.30, running on a Windows 10 enterprise edition. The evaluator also added a non-TOE virtual machine running VEN version 22.2.30 on a windows 10 enterprise edition, to be able to fully test all the TOE's functionalities and their security requirements.

See table 5for the detailed configuration of the TOE components and the testing environment.

Device	Devices information	Purpose
Tested platforms		
PCE	IPv4: 192.168.0.100 MAC: 2C:B8: ED: 33:8a:78 Host Name: PCE	TOE, connected to S1 port 1
VEN 1	IPv4: 192.168.0.101 MAC: 2C:B8: ED:21: A0:1a Host Name: VEN-1	TOE, connected to S1 port 2
Console Server	***BlackBox LES1608A***	***TOE's Console access***
Console server with USB and RJ45 interfaces	Console server with firewall integrated	Provide local console access to TOEs through USB or RJ45 interfaces
LAN switches		
S1	192.168.0.x/24	Switch with port mirroring capability
Virtualized servers		

Device	Devices information	Purpose
Syslog Server	IPv4: 192.168.0.204 MAC: 00:0C:29: f5: E1:37 Host Name: syslog.lab.local	OS: Linux CentOS Stream v8 syslog-ng-3.35.1-1.el9.x86_64 Function: audit server
OpenSSL CA OpenSSL OCSP Responder	IPv4: 192.168.0.208 MAC: 00:0C: 29:2F: 1E:6F Host Name: ca1.lab.local	OS: Linux CentOS Stream v8 Openssl version: OpenSSL 1.0.2k Function: CA and OCSP server
DNS and DHCP server	IPv4: 192.168.0.200 MAC: 00:0C:29:DB: 70:40 Hostname: ad.lab.local	OS: Windows Server 2016 Function: AD, DNS and DHCP servers
NTP Server	IPv4: 192.168.0.206 MAC: 00:0C: 29:5D: F7:E1 Hostname: ntp.lab.local	OS: Linux CentOS Stream v8 NTP version: 4.2.6p5 Function: ntp server
Wireshark VM	SPAN	OS: Linux CentOS Stream v8 Tools/version: Wireshark 2.6.2 (64 bits) Function: Network Traffic Monitor
VEN 2	IPv4: 192.168.0.102 MAC: 2C:B8: ED:24: A0:1a Host Name: VEN-2	Another VEN needed for testing
Management Host (PCE)	IPv4: 192.168.0.162 MAC: 00:0C:29: E4:37: B9 Hostname: mgmt.-1.lab.local	Linux CentOS Stream v8 Bitvise 6.47 and 8.35, putty 0.74, Zennmap v7.93, OpenVAS 22.4.0, Winscp v5.15.2
Management Host (VEN)	IPv4: 192.168.0.157 MAC: 00:0C: 29:CA:81:7B Hostname: mgmt.-2.lab.local	Windows 10 Enterprise Bitvise 6.47 and 8.35, putty 0.74, Zennmap v7.93, , Winscp v5.15.2
Kali Linux	IPv4: 192.168.0.55 MAC: 00:0C:29: A8:3B:2D Hostname: OpenVAS.lab.local	OS: Windows 10 Enterprise Tools version: OpenVAS Pro version 21.4.3

Table 6: TOE's and OE's configuration

2. Security Functional Requirements Evaluation Activities (SFRs)

2.1 TOE Security Specification Evaluation activities (TSS)

2.1.1 Enterprise Security Management (ESM)

2.1.1.1 ESM_ACD.1 Access Control Policy Definition

TSS Assurance Activities:

The evaluator shall do the following:

- *Verify that the TSS identifies one or more compatible Access Control products.*
- *Verify that the TSS describes the scope and granularity of the entities that define policies (subjects, objects, operations, attributes)*
- *Review STs for the compatible Access Control products and verify that there is correspondence between the policies the TOE is capable of creating and the policies the Access Control products are capable of consuming.*
- *Verify that the TSS indicates how policies are identified*

TSS Implementation Details/Results:

The ST, Section 1.3 defines the TOE as *an Enterprise Security Management Policy Management (ESM PM) product*.

(1) The ST Section 7.1 identifies the Virtual Enforcement Node (VEN) as a compatible Access Control product running on Windows operating system and details the policies the VEN is capable of consuming.

(2) The ST Section 7.1.1 describes the scope and granularity of the TOE as follows:

“*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., Windows Firewall), can create, update, or delete a traffic rule targeting inbound, outbound, source IP address, destination IP address, destination port, specific protocol.”

(3) The ST Section 7.1.1 ESM_ACD.1 describes the PCE as an entity that ““*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*.”

(4) Section 7.1.1 of the ST ESM_ACT.1 outlines the policy identification used by the PCE, which can be tracked within the VEN. The PCE assigns a unique version number to each provisioned policy and updates the policy with a new version number each time it is changed. The PCE only maintains one active version of the policy, with previous versions considered historical. New policies provisioned to the VEN come with a unique ID, which can be used to verify that the applied policy version in the VEN is the same as the one currently provisioned on the PCE. To view the policy generation in the VEN, enter the command: "${persistent_data_root}/etc/firewall/debug/sec_policy.generation"

2.1.1.2 ESM_ACT.1 Access Control Policy Transmission

TSS Assurance Activities:

The evaluator shall check the TSS and ensure that it summarizes when and how policy data will be transmitted to Access Control products. This includes the ability to specify the product(s) that the policy data will be sent to.

TSS Implementation Details/Results:

The ST Section 7.1.1 ESM_ACT.1 states that paired VENs poll the PCE a default of every 5 minutes, retrieving policy updates via TLS-protected connections.

The PCE generates policy that the VEN consumes and implements. The VEN is compatible with products specified in Table 3-3: VEN Supported Platforms. All paired VENs periodically connect to the PCE (by default, every 5 minutes) to check for policy updates. All policy updates are sent over a secure channel implemented with TLS.

2.1.1.3 ESM_ATD.1 Object Attribute Definition

TSS Assurance Activities:

The evaluator shall check the TSS to ensure that it describes the object attributes that are defined by the TOE and the purpose for their definition.

TSS Implementation Details/Results:

The ST Section 7.1.1 describes the object attributes and the purpose for their definition.

This section describes the object attributes in terms of labels and workloads, a terminology that is consistently used throughout ST and CC GUIDE. Labels define the type of traffic to be permitted in a new security policy that will apply to one or more paired workloads via the VEN installed on each affected VEN.

The label for a paired workload/platform includes:

- IP address
- Hostname
- OS
- Pairing status for the platform as part of a Workload

The label for the network traffic generated by a paired platform includes:

- Source platform
- Destination platform
- Port the traffic is going to.
- Protocol used by the traffic

2.1.1.4 ESM_EAU.2 Reliance on Enterprise Authentication

TSS Assurance Activities:

The evaluator shall check the TSS in order to determine that it (1) describes the TSF as requiring authentication to use and (2) that it describes, for each type of user or IT entity that authenticates to the TOE, the identification and authentication mechanism that is used. (3)The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each authentication mechanism that is used by the TSF.

TSS Implementation Details/Results:

(1) The ST, Section 7.1.1 states that the TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

(2) The ST, Section 7.1.1 states The TOE users authenticate either locally using direct login, or remotely via a configured domain controller (compatible with SAML) in the operational environment. There are no IT entities that independently authenticate to the TOE, as it initiates communication with the external audit server in order to send audit log entries.

(3) The ST includes two instances of the ESM_EAU.2 SFR, one for local credentials (Section 6.1.1.4) and one for SAML credentials (Section 6.1.1.6).

2.1.1.5 ESM_EID.2 Reliance on Enterprise Identification

TSS Assurance Activities:

This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM_EAU.2.

Please see TSS assurance activity for SFR: ESM_EAU.2

2.1.2 Security Audit (FAU)

2.1.2.1 FAU_GEN.1 Audit Data Generation

TSS Assurance Activities:

The evaluator shall check the TSS and ensure that it summarizes the auditable events and describes the contents of the audit records.

TSS Implementation Details/Results:

The ST Section 7.2, subheading FAU_GEN.1, details audit record generation and includes a description of audit record contents.

"Local audit logs are stored 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 in the event's audit record based upon 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."

2.1.2.2 FAU_SEL_EXT.1 External Selective Audit

TSS Assurance Activities:

The evaluator shall check the TSS in order to determine that it discusses the TSF's ability to configure selective auditing for an Access Control product and that it summarizes the mechanism(s) by which auditable events are selected for auditing.

TSS Implementation Details/Results:

The ST Section 7.2 describes the ability as follows:

"The PCE displays audit events that are reported by managed Workloads (VEN Host id) and Selectable attributes 'Off', 'Allowed', 'Blocked', or 'Allowed+Blocked'."

Description of the three attributes are described in section 7.2 of the Security Target.

2.1.2.3 FAU_STG_EXT.1 External Audit Trail Storage

TSS Assurance Activities:

The evaluator shall check the TSS in order to determine that it describes the location where the TOE stores its audit data, and if this location is remote, the trusted channel that is used to protect the data in transit. The ST author must indicate how audit data is recorded when the external IT entity specified in this requirement is unavailable and how synchronization is achieved when communications are re-established.

If the TOE cannot perform audit reconciliation, then the TSS and the Guidance must explicitly state that there may be a gap in the audit server audit record if the connection between the audit server and ESM product is broken. The TSS must provide a characterization of that loss; further, the Guidance must provide instructions to the administrator on how to configure the ESM product to minimize the loss (e.g., increase local buffer size, inform the administrator of the loss of the connection, etc.).

TD0066 was applied. (https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0066)

TSS Implementation Details/Results:

The ST, Section 7.2 describes how the audit records are protected. Local audit records are stored by the PCE component of the TOE's OS's auditing daemon (rsyslog or syslog-ng). The PCE does not provide functionality that would allow deletion of audit records.

The ST, Section 7.2 states that only authorized administrators, using appropriate host OS commands, may view audit events.

The ST, Section 7.2 explains that the TOE securely forwards audit records to a designated external server over a TLS tunnel. The TLS implementation used by the TOE conforms to the appropriate standards/RFCs and is compliant with the PP specification.

The ST, Section 7.2 explains that the PCE does not perform audit log reconciliation when 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 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. If a syslog connection is broken, an attempt is made to reconnect to the external syslog destination every 60 seconds.

2.1.3 Identification and Authentication (FIA)

2.1.3.1 FIA_AFL.1Authentication Failure Handling

TSS Assurance Activities:

The evaluator shall check the TSS in order to determine that the authentication failure handling function is described in sufficient detail to affirm the SFR.

TSS Implementation Details/Results:

The ST Section 7.3 states that 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. 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.

2.1.3.2 FIA_SOS.1 Verification of Secrets

TSS Assurance Activities:

The evaluator shall check the TSS in order to verify that it discusses the TOE’s strength of secrets capability to a level of detail that is consistent with the SFR.

TSS Implementation Details/Results:

The ST Section 7.3 describes the password attributes, including character set, minimum password length between 16 and 64 characters and password composition rules. For CC evaluated configuration the administrator is required to set the minimum length to 16.

2.1.3.3 FIA_USB.1 User-Subject Binding

TSS Assurance Activities:

The evaluator shall check the TSS in order to determine that it describes the security attributes that are assigned to administrators and the means by which the administrator is associated with these attributes, both during initial assignment and when any changes are made to them.

TSS Implementation Details/Results:

The ST Section 7.3 describes the security attributes that are assigned to administrators and how they are associated with these attributes.

[reference ST Section 7.4 FMT_MOF_EXT.1] Only authorized administrators belonging to appropriate roles (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.

Further the PCE maintains the roles defined in Table 6-4 of the ST. Each authenticated user is automatically associated with a role.

Table 7: 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.
Global Ruleset Provisioner	Provision Rulesets within the All Applications, All Environments, and All Locations scope. They cannot add or modify any Rulesets.
Limited Scope	
Full Ruleset Manager	Add, edit, and delete all Rulesets within the specified scope. Add, edit, and delete Rules when the Provider matches the specified scope The Rule Consumer can match any scope.
Limited Ruleset Manager	Add, edit, and delete all Rulesets within the specified scope. Add, edit, and delete Rules when the Provider and Consumer match the specified scope Cannot manage Rules that use IP Lists, Custom iptables Rules, User Groups, Label Groups, iptables Rules as Consumers, or have Internet connectivity
Ruleset 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. This account cannot be used to login to the Linux OS as it is a system account.

2.1.4 Security Management (FMT)

2.1.4.1 FMT_MOF.1 Management of Functions Behavior

TSS Assurance Activities:

The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it describes the ability of the TSF to perform the required management functions and the authorizations that are required to do this.

TSS Implementation Details/Results:

The ST Section 7.4 describes the ability of the TOE to perform the required management function and details the authorization that are required to do this.

"*The TOE has the ability to determine the behavior of all functions listed in ST, Table 6-3, and restricts them to* "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 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*."

The evaluator reviewed the same section 7.4 of the ST and determined that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s) in the PP PM, page 76.

2.1.4.2 FMT_MOF_EXT.1 External Management of Functions Behavior

TSS Assurance Activities:

The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it summarizes the Access Control product functions that the TOE is able to manage and the authorizations that are required in order to manage these functions.

TSS Implementation Details/Results:

The ST Section 7.4 summarizes the Access Control functions that the TOE manages.

"*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 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.*"

The evaluator found that the above statement from section 7.4 in ST v0.4, is consistent the SFR definition. The first assignment does claim additional function, which is "pair workload", which is mentioned in the above paragraph. The second assignment points back to Table 6-4 in the ST for a list of management functions and roles an administrative user must have to be able to perform them.

2.1.4.3 FMT_MSA_EXT.5 Consistent Security Attributes

TSS Assurance Activities:

The evaluator shall review the TSS and in order to determine that it explains what potential contradictions in policy data may exist.

For example, a policy could potentially contain two rules that permit and forbid the same subject from accessing the same object. Alternatively, the TOE may define an unambiguous hierarchy that makes it impossible for contradictions to occur.

If the TOE does not allow contradictory policy to exist, the evaluator shall verify that this assertion has been made in the TSS and that justification is provided to support the assertion.

TSS Implementation Details/Results:

The ST Section 7.4 states that The TOE (PCE) implements a allow-list access control policy model; consequently, the TOE (PCE) does not allow any contradictory policy to be defined.

Section 7.1.1, Virtual Enforcement Node, states:

- Allow-list model ensures the smallest attack surface by permitting only allowed connections vs. blocking long lists of unauthorized connections.

2.1.4.4 FMT_MTD.1 Management of TSF Data

TSS Assurance Activities:

The evaluator shall review the TSS in order to determine the repository in which the authentication data used by the TOE is stored. The evaluator shall also determine how communications with this repository is secured.

TSS Implementation Details/Results:

For local users, the ST Section 7.4 describes the storage and security of the authentication data.

“*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.*”

For domain users, the ST Section 7.7 describes SAML server interoperability and secure usage.

“*The PCE component of the TOE employs 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*.”

2.1.4.5 FMT_SMF.1 Specification of Management Functions

TSS Assurance Activities:

The evaluator shall check the TSS in order to determine that it summarizes the management functions that are available.

TSS Implementation Details/Results:

The ST Section 6.1.5.5 Table 6-3 identifies the management functions that are implemented by the TOE.

2.1.4.6 FMT_SMR.1 Security Management Roles

TSS Assurance Activities:

The evaluator shall review the TSS to determine the roles that are defined for the TOE. The evaluator shall also review the TSS to verify that the roles defined by this SFR are consistently referenced when discussion how management authorizations are determined.

TSS Implementation Details/Results:

The ST Section 6.1.5.6 Table 6-4 defines the roles for the TOE.

The evaluator verified that roles defined in Section 6.1.5.6 Security Management Roles are consistent with Section 7.4 of the ST.

2.1.5 Protection of the TSF (FPT)

2.1.5.1 FPT_APW_EXT.1 Protection of Stored Credentials

TSS Assurance Activities:

The evaluator shall examine the TSS to determine that it details all authentication data, other than private keys addressed by FPT_SKP_EXT.1, that is used or stored by the TSF, and the method used to obscure the plaintext credential data when stored. This includes credential data stored by the TOE if the TOE performs authentication of users, as well as any credential data used by the TOE to access services in the operational environment (such as might be found in stored scripts).

The TSS shall also describe the mechanisms used to ensure credentials are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.

Alternatively, if authentication data is not stored by the TOE because the authoritative repository for this data is in the Operational Environment, this shall be detailed in the TSS.

TSS Implementation Details/Results:

The ST Section 7.5 describes storage and protection of the credentials. The raw password authentication data are not stored in clear in the non-volatile memory.

“*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 VEN stores secrets in an encrypted file. It uses the Windows DP (Data Protection) API to encrypt and store secrets. Additionally, when login-related configuration information is accessed through regular TOE interfaces, it is obfuscated by substituting the entered password characters with a series of asterisks.

2.1.5.2 FPT_SKP_EXT.1 Protection of Secret Key Parameters

TSS Assurance Activities:

The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.

If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

TSS Implementation Details/Results:

The evaluator examined the ST, section 7.5, that states the following:

"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."

2.1.6 TOE Access (FTA)

2.1.6.1 FTA_SSL.3 TSF-initiated Termination

TSS Assurance Activities:

The evaluator shall check the TSS in order to determine that it discusses how inactivity is handled for remote administrative sessions.

TSS Implementation Details/Results:

The ST Section 7.6 explains that the TOE (PCE) terminates a remote administrative session after an administrator-defined period of inactivity.

2.1.6.2 FTA_SSL.4 User-initiated Termination

TSS Assurance Activities:

The evaluator shall check the TSS in order to determine that it discusses the ability of an administrator to terminate their own session.

TSS Implementation Details/Results:

The ST Section 7.6 discusses that it is possible to terminate (log out) remote administrative sessions.

"*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*."

2.1.6.3 FTA_TAB.1 TOE Access Banner

2.1.6.3.1 TSS Assurance Activities

TSS Assurance Activities:

The evaluator shall check the TSS in order to determine that it discusses the ability of the TSF to display a configurable banner prior to administrator authentication.

TSS Implementation Details/Results:

The ST Section 7.6 discusses a configurable banner implementation.

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

2.1.7 Trusted Path/Channel (FTP)

2.1.7.1 FTP_ITC.1 inter-TSF Trusted Channel

TSS Assurance Activities:

The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

Note: TD0576 https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0576 was applied to this AA.

TSS Implementation Details/Results:

The ST Section 7.7 describe protected communication with IT entities. The TOE uses TLS encapsulation for:

- Traffic that passes between the PCE and each VEN: *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*. Each VEN is identified initially by the administrator-generated key in the pairing process.

- The PCE communicating with an external audit server: The PCE component of the TOE can be configured to export audit records to an external audit server and synchronize with an external authentication server over a secure channel. In order to protect exported audit records and domain authentication data from disclosure or modification, the TOE uses the TLS v1.2 protocol. In both cases, the TOE acts as a client. The external audit server is identified by its assigned X.509v3 certificate.

- web browser-based remote administration of the PCE component of the TOE: *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.*

After the PCE identifies itself to the web browser, the person operating the web browser must still authenticate to the PCE via the Web GUI.

2.1.7.2 FTP_TRP.1 Trusted Path

TSS Assurance Activities:

The evaluator shall check the TSS to ensure that it identifies the protocol(s) used to establish the trusted path and ensure they are consistent with those declared in the ST. In addition, the evaluator shall ensure that the TSS adequately describes the way the trusted communication path is protected.

The evaluator shall also check the TSS to ensure that the ST author specifies whether remote administration is applicable to the TOE and if applicable, specifies all the methods of remote administration, along with how those communications are protected.

Note: TD0576 https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0576 was applied to this AA.

TSS Implementation Details/Results:

The ST Section 7.7 describes protected communication with remote administrators. The TOE uses TLS for web-based administration.

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

After the PCE identifies itself to the web browser, the person operating the web browser must still authenticate to the PCE via the Web GUI.

2.2 Guidance Requirements Evaluation Activities (AGD)

2.2.1 Enterprise Security Management (ESM)

2.2.1.1 ESM_ACD.1 Access Control Policy Definition

2.2.1.1.1 Guidance Assurance Activities

Guidance Assurance Activities: *The evaluator shall review the operational guidance to ensure that that it indicates the compatible Access Control product(s) as well as the allowable contents and means of identification of the access control policies that can be defined by the TOE.*

Guidance Implementation Details/Results:

The evaluator reviewed CC GUIDE, chapter 1, Section "Target of Evaluation (TOE)" and noted that the Virtual Enforcement Node (VEN) is identified as an Access Control product that is compatible with the TOE.

Additionally, the evaluator noted that chapter 7, Section "Visualizing Policy" describes access control policies, their creation with the PCE component of the TOE, and their enforcement by the VEN component of the TOE.

The PCE Illumination feature reveals the relationships between Workloads and provides Workload context (OS, running services, and open TCP ports) to the Policy Compute Engine (PCE). It monitors traffic passing between Workloads, determines their relationships, draws a graph of the interactions between the Workloads, and then visualizes them into Groups. Once the relationships between Workloads are understood, it can be labelled, and policies created which lead to enforcement.

Enforcement ensures secure relationships between Workloads. Using the graph of dependencies between Workloads—based on the Labels assigned to the Workloads and the created Rules—the PCE computes and deploys a security policy to each Workload. The VEN on the Workload then configures the native OS to enforce the security policy.

CC Guide (February), Chapter 6, page 116 describes policy identification: "Policies are identified using unique policy ID numbers. The policy ID identifies the policy and (if applicable) the version of the policy." With reference to the CC Scope, Chapter 7 includes a box with "NOTE: This section is provided for informational purposes only. Visualizing policy is outside the scope of the Common Criteria evaluation. Also, outside the scope is the translation of rules by the VEN. The scope of this evaluation includes policy definition and transmission of policies from PCE to VEN."

2.2.1.2 ESM_ACT.1 Access Control Policy Transmission

2.2.1.2.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall review the operational guidance to determine how to create and update policies, and the circumstances under which new or updated policies are transmitted to consuming ESM products (and how those circumstances are managed, if applicable).

Guidance Implementation Details/Results:

The evaluator reviewed CC GUIDE, chapter 7 and noted that it provides:

- An introduction to how the TOE uses policies, and basic concepts such as Workloads.
- How labels work for quantifying relationships between Workloads
- Assigning labels to Workloads
- Pairing VENs, or installing a VEN on a specific Workload
- Configuring a VEN to examine, ignore, test, and enforce the PCE allow-list model on a Workload.

The CC GUIDE, chapter 7 reiterates the concept that a VEN in enforced mode will block all traffic to/from a Workload that is not listed as a Rule in the PCE allow-list for that specific VEN.

The CC GUIDE, section “VEN and policy updates” in chapter 7, details the circumstances under which new or updated policies are transmitted to the VEN, by stating the following:” The VEN receives notifications about policy updates from the PCE in two ways:

o The VEN sends a heartbeat message every 5 minutes to the PCE, and the PCE responds to the message with any updates for the VEN (for example, a new policy update is waiting for the VEN).

o The VEN opens a persistent connection with the PCE (called Event Channel), and the PCE sends notifications over that channel.

When a VEN is configured from Idle to Enforcement or Visibility mode, the VEN uses whatever policy it receives from the PCE.”

2.2.1.3 ESM_ATD.1 Object Attribute Definition

2.2.1.3.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall check the operational guidance to ensure that it provides instructions on how to define and configure the object attributes.

Guidance Implementation Details/Results:

CC GUIDE chapter 7, section “introduction to core policy” explains policies that get created by the PCE and enforced by one or more VENs. This section provides basic instructions on creating labels, thereby defining and configuring the object attributes needed for the TOE in creating a security policy.

2.2.1.4 ESM_EAU.2 Reliance on Enterprise Authentication

2.2.1.4.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall (1) check the operational guidance in order to determine how the TOE determines whether an interactive user requesting access to it has been authenticated and (2) how the TOE validates authentication credentials or identity assertions that it receives.

If any IT entities authenticate to the TOE, the evaluator shall also check the operational guidance to (3) verify that it identifies how these entities are authenticated and (4) what configuration steps must be performed in order to set up the authentication.

Guidance Implementation Details/Results:

(1) The CC GUIDE, chapter 4, Section 1 adequately describes all authentication methods. The TOE can use local credentials provided by PCE, or domain credentials provided by ADFS [Active Directory Federation Service] as a SAML provider.

(2) The CC GUIDE, chapter 4, Section 1 details the process of authenticating a local user. The user must provide a username and password in order to login locally. The CC GUIDE, chapter 4, Section "SAML SSO Authentication" details the process of authentication using SAML protocol. When using local login, user credentials are checked against the internal authorized users database. When using domain login, the TOE initiates an authentication request to the external domain controller (AD) using SAML, and only allows access after receiving a successful result message.

(3) No IT entities authenticate to either component of the TOE.

(4) Not applicable as per (3).

2.2.1.5 ESM_EID.2 Reliance on Enterprise Identification

2.2.1.5.1 Guidance Assurance Activities

Guidance Assurance Activities:

This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM_EAU.2.

Please see guidance assurance activity for SFR: ESM_EAU.2

2.2.2 Security Audit (FAU)

2.2.2.1 FAU_GEN.1 Audit Data Generation

2.2.2.1.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit record.

Each audit record format type shall be covered and shall include a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 3.

The evaluator shall review the operational guidance, and any available interface documentation, in order to determine the administrative interfaces (including subcommands, scripts, and configuration files) that permit configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP.

The evaluator shall document the methodology or approach taken to do this. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements. Using this list, the evaluation shall confirm that each security relevant administrative interface has a corresponding audit event that records the information appropriate for the event.

Guidance Implementation Details/Results:

The evaluator checked all guidance documents, as listed in the Security Target Section 3.4 Table 3-5. Each TOE platform is accompanied by the following guidance documents:

- Illumio Core Platform 22.2.30 PCE Operations
- Illumio Core Platform 22.2.30 PCE Deployment Guide
- Illumio Core Platform Common Criteria Guide v22.2.30

The TOE implements an administrative interface over HTTPS/TLS that supports all management functions and generates appropriate audit events.

Note that Auditing is started when PCE is started and closed when PCE is shutdown. There are no separate events to indicate audit start or shutdown.

The full list of auditable events and guidance location is in the following table:

Table 8: Auditable events to guidance coverage.

Requirement	Auditable Events	Guidance Location
ESM_ACD.1	Creation or modification of policy	CC GUIDE – Chapter 8 – Auditable Events
ESM_ACT.1	Transmission of policy to Access Control products	CC GUIDE – Chapter 8 – Auditable Events
ESM_ATD.1	Definition of object attributes	CC GUIDE – Chapter 8 – Auditable Events
ESM_EAU.2	All use of the authentication mechanism	CC GUIDE – Chapter 8 – Auditable Events
FAU_SEL_EXT.1	All modifications to audit configuration	CC GUIDE – Chapter 8 – Auditable Events
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	CC GUIDE – Chapter 8 – Auditable Events
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold	CC GUIDE – Chapter 8 – Auditable Events
	the actions taken when the threshold is reached	

	any actions taken to restore the normal state	
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret	CC GUIDE – Chapter 8 – Auditable Events
FMT_SMF.1	Use of the management functions	CC GUIDE – Chapter 8 – Auditable Events
FMT_SMR.1	Modifications of the management roles	CC GUIDE – Chapter 8 – Auditable Events
FTA_SSL.3	All session timeout events	CC GUIDE – Chapter 8 – Auditable Events
FTA_SSL.4	All session termination events (logouts)	CC GUIDE – Chapter 8 – Auditable Events
FTP_ITC.1	All use of trusted channel functions	CC GUIDE – Chapter 8 – Auditable Events
FTP_TRP.1	All attempted uses of the trusted path functions	CC GUIDE – Chapter 8 – Auditable Events
FAU_GEN.1	Startup and shutdown of the system	CC GUIDE – Chapter 8 – Auditable Events

The following management functions were identified in the PP as security-relevant. These functions are documented in the user guidance and noted to generate appropriate audit events:

Requirement	Auditable Events	Guidance Location
ESM_ACD.1	Creation or modification of policy	CC GUIDE – Chapter 8 – Auditable Events
ESM_ACT.1	Transmission of policy to Access Control products	CC GUIDE – Chapter 8 – Auditable Events
ESM_ATD.1	Definition of object attributes	CC GUIDE – Chapter 8 – Auditable Events
ESM_EAU.2	All use of the authentication mechanism	CC GUIDE – Chapter 8 – Auditable Events
FAU_SEL_EXT.1	All modifications to audit configuration	CC GUIDE – Chapter 8 – Auditable Events
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	CC GUIDE – Chapter 8 – Auditable Events
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold	CC GUIDE – Chapter 8 – Auditable Events
	the actions taken when the threshold is reached	
	any actions taken to restore the normal state	
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret	CC GUIDE – Chapter 8 – Auditable Events
FMT_SMF.1	Use of the management functions	CC GUIDE – Chapter 8 – Auditable Events
FMT_SMR.1	Modifications of the management roles	CC GUIDE – Chapter 8 – Auditable Events
FTA_SSL.3	All session timeout events	CC GUIDE – Chapter 8 – Auditable Events
FTA_SSL.4	All session termination events (logouts)	CC GUIDE – Chapter 8 – Auditable Events
FTP_ITC.1	All use of trusted channel functions	CC GUIDE – Chapter 8 – Auditable Events
FTP_TRP.1	All attempted uses of the trusted path functions	CC GUIDE – Chapter 8 – Auditable Events

CC GUIDE is the key document that contains explanations of security-relevant features and details secure. configurations. The TOE security functionality is identical across all platforms, and as a result, this document is applicable to all TOE platforms and hardware configurations. CC GUIDE provides single source and easy-to-follow instructions on how to put the TOE into evaluated configuration, effectively minimizing the possibility of end-user misunderstanding and TOE misconfiguration. This guide was closely followed during product testing and was found to be an accurate and useful source of information.

As related to Security Audit, CC GUIDE Chapter 3, Section "Syslog Forwarding" explains that auditing is configur by default, and that in the evaluated configuration an external audit server must also be configured. Chapter 3, Section "Event Settings in PCE Web Console" explains how to configure logging format. Chapter 8, Section "Eve Syntax" provides an explanation of the audit log record format, and audit records to individual SFRs.

During testing, the evaluator confirmed that the information in CC GUIDE is accurate, and the examples are representative of a typical scenario encountered by the end-users.

2.2.2.2 FAU_SEL_EXT.1 External Selective Audit

2.2.2.2.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events and shall confirm that it contains all of the selections identified in the Security Target.

Guidance Implementation Details/Results:

The evaluator reviewed CC GUIDE, chapter 6, Section "Enforcement mode for Policy", which describes the three selectable attributes [Off, Blocked, Allowed+Blocked] captured in the VEN and displayed by selection thru visibility feature in the PCE for a specific VEN (host identifier)

2.2.2.3 FAU_STG_EXT.1 External Audit Trail Storage

2.2.2.3.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall check the operational and preparatory guidance in order to determine that they describe how to configure and use an external repository for audit storage. The evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established.

If the TOE cannot perform audit reconciliation, then the TSS and the Guidance must explicitly state that there may be a gap in the audit server audit record if the connection between the audit server and ESM product is broken. The TSS must provide a characterization of that loss; further, the Guidance must provide instructions to the administrator on how to configure the ESM product to minimize the loss (e.g., increase local buffer size, inform the administrator of the loss of the connection, etc.).

TD0066 was applied. (https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0066)

Guidance Implementation Details/Results:

Chapter 3, Section “Syslog Forwarding” of the CC GUIDE documents the necessary steps for configuring the TLS protocol between the TOE and the external audit server.

1) Configuring a connection for the external audit server as an additional repository, providing all relevant information to connect, including an X.509v3 certificate for mutual authentication.
2) Indicating what level of detail is to be sent to the external audit server.
3) Saving the new connection and waiting for the PCE to establish the connection.

The TOE logs consolidation for period of time depending on the level of configured severity, however for a log network outage, the PCE has the capability to detect the loss of log messages that should be forwarded to syslog remote destinations. The PCE maintains a queue of log messages to be forwarded. 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.

2.2.3 Identification and Authentication (FIA)

2.2.3.1 FIA_AFL.1Authentication Failure Handling (review)

2.2.3.1.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall check the operational guidance to verify that a discussion on authentication failure handling is present and consistent with the representation in the Security Target.

Guidance Implementation Details/Results:

The evaluator reviewed CC GUIDE Section “How and When the PCE Locks Out Users” and noted that it describes the threshold value for a number of unsuccessful authentication attempts. The first sentence in this section states:

“By default, the PCE enforces the following login lockout behavior:

- Lockout value after invalid login attempts

After a user enters an invalid password 5 consecutive times while attempting to log into the PCE, the user's account is locked for 15 minutes. The login lockout feature resets the account after 15 minutes and does not require an Illumio administrator to unlock it. The number of unsuccessful authentication attempts can be configured by changing the default value of the runtime variable max_failed_login_attempts (default: 5; minimum: 1; maximum: 256) in the configuration file runtime_env.yml. Similarly, the lockdown period can be configured by changing the default value of account_lockout_duration_minutes (default: 15; minimum: 1; maximum: 256).”

2.2.3.2 FIA_SOS.1 Verification of Secrets

2.2.3.2.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall check the operational guidance in order to verify that it provides information to administrators about the TOE's enforcement of password composition, reuse, and aging or of a non-password-based credential.

If the TOE does not support password-based credentials, the evaluator shall check to verify that the operational guidance provides information about the credential that is used by the TSF and how it is supplied to the TOE.

The evaluator shall also check the operational guidance to verify that it discusses the aspects of the strength of secrets policy that can be configured and what steps an administrator needs to perform in order to configure it.

Guidance Implementation Details/Results:

The evaluator reviewed CC GUIDE, Chapter 4, Section "Password Policy Configuration" and noted that it describes the settings of the password policy. Also, the PCE GUIDE, chapter 7, section "Password Policy Configuration" provides more information about how the TOE handles the enforcement of password policy. As per the previous section, The Password Policy feature is not applicable for organizations using SAML authentication. The PCE GUIDE, chapter 7, Section "password requirements", states the following "The password requirements you set are displayed to users when they are required to change their passwords. You can set the minimum character length, ranging from a minimum of 8 characters to a maximum of 64 characters. The default length is 8 characters.

A Global Organization Owner should configure passwords based on the following categories:

- Uppercase English letters
- Lowercase English letters
- Numbers 0 through 9 inclusive
- Any of the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "?", ">","<"

You have to select at least three of the above categories. The default password requirement is one number, one uppercase character, and one lowercase character. You can set the password to use either one or two characters from each category.

For Common Criteria evaluated configuration, the administrator is required to set the minimum length to 16."

2.2.3.3 FIA_USB.1 User-Subject Binding

2.2.3.3.1 *Guidance Assurance Activities*

Guidance Assurance Activities:

The evaluator shall check the operational guidance in order to verify that it describes the mechanism by which external data sources are invoked and mapped to user data that is controlled by the TSF.

Guidance Implementation Details/Results:

The section 2.2.3.3.1 of AAR v0.4 was updated to indicate that the evaluator reviewed Chapter 5, Section "User Management" of the CC GUIDE, specifically the subsections "Add or Remove an External User" and "Add or Remove an External Group." These subsections clearly outline the process for invoking and mapping external data sources to user data for all roles. The sections describe the creation of external users, the assignment of roles to these users, the setup of access-controlled users, and the addition and deletion of both external users and groups. The subsections demonstrate how external users are created, linked to roles, and able to perform their designated activities.

2.2.4 Security Management (FMT)

2.2.4.1 FMT_MOF.1 Management of Functions Behavior

2.2.4.1.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall review the operational guidance in order to determine what restrictions are in place on management of these attributes and how the TSF enforces them. For example, if management authority is role-based, then the operational guidance shall indicate this.

Guidance Implementation Details/Results:

The evaluator reviewed CC GUIDE, Chapter 5, Sections “User Management” and “About Roles, Scopes, and Granted Access” and noted that they describe how the PCE component of the TOE restricts access to management functions (e.g., role-based access control).

The following table, created from cross-referencing the tables in CC GUIDE – Chapter 8 – Auditable Events and Chapter 3, Section “Management Functions”, details management functions and the authorized role for each management function.

Requirement	Management Function	Authorized Role
ESM_ACD.1	Creation of policies	Global Organization Owner Global Administrator
ESM_ACT.1	Transmission of policies	Global Organization Owner Global Administrator
ESM_ATD.1	Definition of object attributes	Global Organization Owner Global Administrator
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	Global Organization Owner
FAU_SEL.1	Configuration of auditable events	Global Organization Owner Global Administrator
FAU_SEL_EXT.1	Configuration of auditable events for defined external entities	Global Organization Owner Global Administrator
FAU_STG_EXT.1	Configuration of external audit storage location	Global Organization Owner Global Administrator
FIA_AFL.1	Configuration of authentication failure threshold value	Global Organization Owner Global Administrator
	Configuration of actions to take when threshold is reached	Global Organization Owner Global Administrator

	Execution of restoration to normal state following threshold action	Global Organization Owner Global Administrator
FIA_SOS.1	Management of the metric used to verify secrets	Global Organization Owner Global Administrator
FMT_MTD.1	Management of user authentication data	Global Organization Owner
FMT_SMR.1	Management of the users that belong to a particular role	Global Organization Owner
FTA_TAB.1	Maintenance of the banner	Global Organization Owner Global Administrator
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	Global Organization Owner Global Administrator
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	Global Organization Owner Global Administrator

2.2.4.2 FMT_MOF_EXT.1 External Management of Functions Behavior

2.2.4.2.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall check the operational guidance in order to determine that it provides instructions for how to connect to an Access Control product and what privileges are required to perform management functions on it once the connection has been established.

Guidance Implementation Details/Results:

The evaluator reviewed CC GUIDE, chapter 5, Chapter 6, Section "Pairing VENs" and then referenced VEN GUIDE pages 08-10, noting that between the two, they describe how the PCE and VEN components of the TOE connect via pairing. The following table, based on CC GUIDE chapter 5, section "User Management", details the roles and their allowed management function on the VEN**.**

Access Control Product	Management Function	Authorized Role
VEN	Pairing a workload	Global Organization Owner Global Administrator

2.2.4.3 FMT_MSA_EXT.5 Consistent Security Attributes

2.2.4.3.1 Guidance Assurance Activities

Guidance Assurance Activities:

If the TOE requires manual intervention in order to resolve contradictory policy data, the evaluator shall review the operational guidance in order to verify that it provides a summary of contradictory policy situations and the steps that must be taken in order to resolve them.

If the TOE's policy engine prevents such contradictions, the evaluator shall review the operational guidance in order to verify that it describes how the TSF reconciles any contradictory policy data (such as different rules simultaneously allowing and denying a certain behavior).

Guidance Implementation Details/Results:

The evaluator reviewed CC GUIDE, Chapter 7, *Section "Components of Core Policy" and* noted it describes how the TOE's policy engine prevent contradictions and it describes how any contradictory policy is reconciled.

"*Because the PCE employs an allow-list policy model, it is not possible for contradictory rules to be created. Before any rules are written, all traffic 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.*"

2.2.4.4 FMT_MTD.1 Management of TSF Data

2.2.4.4.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall review the operational guidance in order to determine that it includes the data that can be managed and who is able to manage this data. This can be separated over multiple roles to distinguish between user administration and self-service; for example, both a Security Administrator and a specific user may be able to modify that user's own password.

Guidance Implementation Details/Results:

The evaluator reviewed CC GUIDE, Chapter 5, Section "About Roles, Scopes, and Granted Access", and the table provided in that section maps the role to the managed authentication data.

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 Provisioner	Provision Rulesets within specified scope
Ruleset Viewer	View rules that match the scope. Cannot edit rulesets or rules.
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.

The permission of interest in the above table is “user account”. Only the Global Organization Owner role can make changes.

2.2.4.5 FMT_SMF.1 Specification of Management Functions

2.2.4.5.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall check the operational guidance in order to determine that it defines all of the management functions that can be performed against the TSF, how to perform them, and what they accomplish.

Guidance Implementation Details/Results:

The evaluator reviewed the CC GUIDE Chapter 3, Section “Management Function” and noted that all management functions are described. They are mapped in the table below:

Requirement	Management Function	Guidance
ESM_ACD.1	Creation of policies	CC GUIDE – Chapter 7
ESM_ACT.1	Transmission of policies	CC GUIDE – Chapter 7
ESM_ATD.1	Definition of object attributes	CC GUIDE – Chapter 7
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	CC GUIDE – Chapter 4, section “Authentication”
FAU_SEL.1	Configuration of auditable events	CC GUIDE – Chapter 3, section “Configuring Event Audit Levels”
FAU_SEL_EXT.1	Configuration of auditable events for defined external entities	CC GUIDE – Chapter 3, section “Event Severity Levels”

FAU_STG_EXT.1	Configuration of external audit storage location	CC GUIDE – Chapter 3, section “Forward Events to External Syslog Server”
FIA_AFL.1	Configuration of authentication failure threshold value	CC GUIDE – Chapter 4, Section “How and When the PCE Locks Out Users”
	Configuration of actions to take when threshold is reached	CC GUIDE – Chapter 4, Section “How and When the PCE Locks Out Users”
	Execution of restoration to normal state following threshold action	CC GUIDE – Chapter 4, Section “How and When the PCE Locks Out Users”
FIA_SOS.1	Management of the metric used to verify secrets	CC GUIDE – Chapter 4, section “Password Policy Configuration”
FMT_SMR.1	Management of the users that belong to a particular role	CC GUIDE – Chapter 5, section “Setup for Role-based Access Control”
FTA_TAB.1	Maintenance of the banner	CC GUIDE - Chapter 1, section “Assumptions and Operational Environment”
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	CC GUIDE – Chapter 2, section “X.509 Certificate”
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	CC GUIDE – Chapter 2, section “X.509 Certificate”

The banner message is set through a configuration file used at the start of PCE. The evaluator changed the banner text and restarted the PCE to verify that the updated banner text is displayed.

2.2.4.6 FMT_SMR.1 Security Management Roles

2.2.4.6.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall review the operational guidance in order to verify that it provides instructions on how to assign users to roles. If the TSF provides only a single role that is automatically assigned to all users, then the evaluator shall review the operational guidance to verify that this fact is asserted.

Guidance Implementation Details/Results:

The evaluator reviewed CC GUIDE Chapter 5, section “Setup for Role-based Access Control” and noted it describes how to assign roles to users, which is the same action as assigning a user to a role.

2.2.5 Protection of the TSF (FPT)

2.2.5.1 FPT_APW_EXT.1 Protection of Stored Credentials

2.2.5.1.1 Guidance Assurance Activities

Guidance Assurance Activities: None

Guidance Implementation Details/Results: N/A

2.2.5.2 FPT_SKP_EXT.1 Protection of Secret Key Parameters

2.2.5.2.1 Guidance Assurance Activities

Guidance Assurance Activities: None
Guidance Implementation Details/Results: N/A

2.2.6 TOE Access (FTA)

2.2.6.1 FTA_SSL.3 TSF-initiated Termination

2.2.6.1.1 Guidance Assurance Activities

Guidance Assurance Activities: *The evaluator shall also check the operational guidance in order to verify that it describes how to set the idle time threshold.*
Guidance Implementation Details/Results: The evaluator checked CC GUIDE Chapter 4, section “Configure Session Timeout” and verified that it describes how to set the inactivity timer for remote administrative sessions.

2.2.6.2 FTA_SSL.4 User-initiated Termination

2.2.6.2.1 Guidance Assurance Activities

Guidance Assurance Activities: *The evaluator shall check the operational guidance in order to verify that it describes how an administrator can terminate their own administrative session for each administrative interface that is supported by the TOE.*
Guidance Implementation Details/Results: The evaluator reviewed CC GUIDE Chapter 2, Section “Log Out” and verified that it describes how to terminate administrative sessions.

2.2.6.3 FTA_TAB.1 TOE Access Banner

2.2.6.3.1 Guidance Assurance Activities

Guidance Assurance Activities: *The evaluator shall review the operational guidance to determine how the TOE banner is displayed and configured.*
Guidance Implementation Details/Results: The evaluator reviewed CC GUIDE Chapter 2, section “Configure PCE as a SNC (Single Node Cluster) and noted that it does describes steps to configure the TOE banner as part of configuring the PCE component of the TOE.

2.2.7 Trusted Path/Channel (FTP)

2.2.7.1 FTP_ITC.1 inter-TSF Trusted Channel

2.2.7.1.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

Note: TD0576 https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0576 was applied to this AA.

Guidance Implementation Details/Results:

The evaluator reviewed the CC GUIDE Chapter 6, section "X.509 Requirements" and noted that it describes the PCE's side of configuring TLS sessions with VENs, the external audit server, and remote administrators connecting via web browsers.

CC GUIDE Chapter 3, section "Configuring Remote Audit Server with TLS" go into detail for the external audit server configuration, whereas the two other connection types are automatic and not configurable beyond steps performed in Chapter 3, section "Configuring Event Audit Levels.

As per CC GUIDE Chapter 3, section "Syslog Forwarding", the PCE continually logs audit messages, so when a network connection is restored to the external audit server after having been broken, unsent log messages are then sent.

2.2.7.2 FTP_TRP.1 Trusted Path

2.2.7.2.1 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall confirm that the guidance documentation contains instructions for how users will interact with the TOE such as a web application via HTTPS. The evaluator shall also ensure that the guidance documentation discusses the mechanism by which a trusted path to the TOE is established and which environmental components (if any) the TSF relies on to assist in this establishment.

If remote administration is applicable to the TOE per the TSS, the evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.

Note: TD0576 https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0576 was applied to this AA.

Guidance Implementation Details/Results:

The evaluator reviewed the PCE GUIDE Chapter 6, section " Certificate Requirements" and noted that it describes the PCE's side of configuring TLS sessions with VENs, the external audit server, and remote administrators connecting via web browsers.

Chapter 3, section "Configuring Remote Audit Server with TLS" goes into detail for the external audit server configuration. Chapter 2, section "How to Access Your System" explains how a remote administrator accesses the PCE Web GUI.

2.3 Testing Requirements Evaluation Activities (ATE)

2.3.1 Enterprise Security Management (ESM)

2.3.1.1 ESM_ACD.1 Access Control Policy Definition

2.3.1.1.1 Testing Assurance Activities

Testing Assurance Activities:

a) The evaluator shall test this [Access Control policy] capability by using the TOE to create a policy that uses the full range of subjects, objects, operations, and attributes and sending it to a compatible Access Control product for consumption.
b) The evaluator will then perform actions that are mediated by the Access Control product in order to confirm that the policy was applied appropriately.
c) The evaluator will also verify that a policy identifier is associated with a transmitted policy by querying the policy that is being implemented by the Access Control product.

Testing Implementation Details/Results:

a) and b): The evaluator created and provisioned different rules using all the objects/subjects, corresponding tp different attributes mentioned in the SFR: ESM_ACD.1, as following:

- Subjects: [***platform handler (workload)***]
- Objects: [***network traffic filter***]; and
- Operations: [***create, update, delete***]; and
- Attributes: [***inbound, outbound, src IP, dst IP, dst port, protocol***].

The evaluator created VENs and other workloads, like AD server or VEN-2 using all the possible network traffic filters and applied using different combinations of (source IP, destination IPs, destination ports, and protocol). The evaluator created, updated PCE rules and provisioned these policies to be consumed by workloads and VENs. The evaluator noticed that the VEN was allowing or disallowing traffic based on configured attributes (inbound, outbound traffics source and destination addressed or protocols) in the rule polices. The evaluator deleted a policy and provisioned the new change to the workloads and noticed that behavior change manifested by the VEN. The TOE behaved as expected on using every object, subjects, operations, and attributes and enforced every policy.

Test results for a) and b): PASS

c): For each of the test policies in a) and b), the evaluator observed that the policy identifier was present in the Web GUI for the PCE component of the TOE, confirmed successful transmission of an updated unified security policy to the VEN, and that the VEN behaved as expected afterwards.

Test c) result: PASS

2.3.1.2 ESM_ACT.1 Access Control Policy Transmission

2.3.1.2.1 Testing Assurance Activities

Testing Assurance Activities:

The evaluator shall test this [Policy Transmission] capability by obtaining one or more compatible Access Control products and configuring the TOE to manage them. Then,

Test 1: following the procedures in the operational guidance for both the TOE and the Access Control product, the evaluator shall create a new policy and ensure that the new policy defined in the by the TSF is successfully transmitted to, consumed by, and enforced in an Access Control product, in accordance with the circumstances defined in the SFR. In other words,

a) if the selection is completed to transmit after creation of a new policy, then the evaluator shall create the new policy and ensure that, after a reasonable window for transmission, the new policy is installed;

b) if the selection is completed to transmit periodically, the evaluator shall create the new policy, wait until the periodic interval has passed, and then confirm that the new policy is present in the Access Control component; or

c) if the section is completed to transmit upon the request of a compatible Secure Configuration

Management component, the evaluator shall create the policy, use the Secure Configuration Management component to request transmission, and the confirm that the Access Control component has received and installed the policy. If the ST author has specified "other circumstances", then a similar test shall be executed to confirm transmission under those circumstances.

Test 2: The evaluator shall then make a change to the previously created policy and then repeat the previous procedure to ensure that the updated policy is transmitted to the Access Control component in accordance with the SFR-specified circumstances.

Test 3: Lastly, as updating a policy encompasses deletion of a policy, the evaluator shall repeat the process a third time, this time deleting the policy to ensure it is removed as an active policy from the Access Control component.

Test 4: The evaluator shall repeat this test for a representative sample of Access Control products that can be managed by the TOE. For example, if the TOE provides the ability to manage groups of host-based access control endpoints, the evaluator shall create different groups such that each supported platform is included in at least one group and verify that group members will appropriately consume policies when instructed to do so.

Note: This testing will likely be performed in conjunction with the testing of ESM_ACD.1.

Testing Implementation Details/Results:

Test 1: The evaluator created a new policy that was acceptable to thet allow-list model maintained by the PCE. The VEN then automatically pulled its own updated and personalized security policy from the PCE.

a) The PCE automatically signals the affected workload to update its individualized firewall rules when a new policy that affects said workload clears the allow-list model.

b) During the testing activity, the evaluator noticed that the VEN will poll the PCE automatically for firewall rule updates whenever it paires with the PCE or comes back online.

c) This is not applicable; therefore, it was not tested.

Test 1 result: PASS

Test 2: The evaluator changed part of how the policy behavior, observed the updated policy being retrieved by the VEN, and tested the functionality to verify that the VEN enforced the change.

Test 2 result: PASS

Test 3: The evaluator deleted the policy, observed the updated policy being retrieved by the affected VENs, then tested the functionality to verify that the policy was no longer being enforced.

Test 3 result: PASS

Test 4: This is not applicable as the only applicable ACP is the VEN, and it has been tested as per above.

Test 4 result: PASS

2.3.1.3 ESM_ATD.1 Object Attribute Definition

2.3.1.3.1 Testing Assurance Activities

Testing Assurance Activities:

The evaluator shall test this capability by creating a policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy.

Testing Implementation Details/Results:

This is addressed by the following test from section 2.1.1.3 of this AAR:

The evaluator:

1. created two test policies using labels as defined attributes (one to permit sending a ping between two workloads, and one to permit a remote ping of a VEN)
2. tested the functionality prior to provisioning each policy, applied each to one of two separate paired VENs / Workloads
3. observed each policy being transmitted.
4. confirmed that each policy was applied appropriately by testing functionalities between the host systems (Workloads) for the VENs

Test result: PASS

2.3.1.4 ESM_EAU.2 Reliance on Enterprise Authentication

Testing Assurance Activities:

The evaluator shall…

(1) test this capability [Enterprise Authentication] by accessing the TOE without having provided valid identification and authentication information and observe that access to the TSF is subsequently denied.

(2) If any IT entities authenticate to the TOE, the evaluator shall instruct these IT entities to provide invalid identification and authentication information and observe that they are not able to access the TSF.

Testing Implementation Details/Results:

(1) The evaluator provided both invalid and valid local and SAML-Based login credentials to access the PCE component of the TOE and observed that access to the TSF was denied or permitted depending on the validity of the credential used.

(2) This assurance activity is already addressed in test 3 in Section 2.3.3.2 FIA_SOS.1 Verification of Secrets of this document.

Test result: PASS

2.3.1.5 ESM_EID.2 Reliance on Enterprise Identification

Testing Assurance Activities:

This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM_EAU.2.

Testing Implementation Details/Results:

Please see testing assurance activity for SFR: ESM_EAU.2

2.3.2 Security Audit (FAU)

2.3.2.1 FAU_GEN.1 Audit Data Generation

Testing Assurance Activities:

Test 1: The evaluator shall test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities.

Test 2: The evaluator shall then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST.

This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs is consistent with the activity performed on the TOE. For example, if a test is performed such that a policy is defined, the corresponding audit record should correctly identify the policy that was defined.

Testing Implementation Details/Results:

Test 1: The evaluation team confirmed, as part of testing activities, that appropriate audit records were generated, and that each audit record contained appropriate and accurate information. The following maps requirements to events and test cases.: The description and details of the test cases are available in a separate proprietary Test Report and may be obtained by contacting Illumio.

Requirement	Auditable Events	Test Case
ESM_ACD.1	Creation or modification of policy	PP-1D, PP-1B
ESM_ACT.1	Transmission of policy to Access Control products	PP-1D, PP-1B
ESM_ATD.1	Definition of object attributes	PP-1D, PP-1B
ESM_EAU.2	All use of the authentication mechanism	PP-2A, PP-2B

FAU_SEL_EXT.1	All modifications to audit configuration	PP-3G
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	PP-3A, PP-3D, PP-14A
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	PP-2A
FIA_SOS.1	Rejection or acceptance by the TSF of any tested secret	PP-5A, PP-5B, PP-5D, PP-5E, PP-5F, PP-5H
	The change made to the quality metric	
	Identification of any changes to the defined quality metrics	
FMT_SMF.1	Use of the management functions, Management function performed	PP-1B, PP-1D, PP-3A, PP-5H, PP-7, PP-8, PP-10, PP-12
FMT_SMR.1	Modifications of the management roles	PP-7
FTA_SSL.3	All session timeout events	PP-12B
FTA_SSL.4	All session termination events (logouts)	PP-2A, PP-2B, PP-3A, PP-7, PP-8
FTP_ITC.1	All use of trusted channel functions	PP-14A, PP-14C, PP-3D
FTP_TRP.1	All attempted uses of the trusted path functions	PP-14B
FAU_GEN.1	Startup and shutdown of the system	PP-3A

The detailed steps of the tests performed are described in a separate proprietary Test plan. Contact Illumio https://www.illumio.com/contact-us for access.

Test result: PASS

Test 2: in every test case, the evaluator checked the local audit event repository and found that an appropriate audit event was generated, and it contained the attributes as defined by the ST.

Test result: PASS

2.3.2.2 FAU_SEL_EXT.1 External Selective Audit

Testing Assurance Activities:

The evaluator shall test this capability by configuring a compatible Access Control product to have:

- *All selectable auditable events enabled.*
- *All selectable auditable events disabled.*
- *Some selectable auditable events enabled.*

For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded by the Access Control product.

Testing Implementation Details/Results:

In visibility mode (on the PCE), the level of detail provided by each operational VEN is Blocked, Blocked + Allowed, or Off.

For a specific host of the VEN:

- The visibility mode in VEN was set to send event logs for “Blocked + Allowed” traffic, then the evaluator generated network traffic between workloads and VENs and confirmed the correct behavior of the VENs.
- VEN2 was set to generate event logs for ‘blocked’ network traffic only, which resulted in not seeing VEN logs for ‘Allowed’ network traffic.
- The visibility mode, in VEN2 properties was turned ‘Off’, which resulted in not seeing any of logs of blocked or allowed network traffic.
- In the end, the evaluator configured different attributes on each host identity (VEN1 and VEN2) and determined that each VEN only displayed the attributes that had been selected for it.

Test result: PASS.

2.3.2.3 FAU_STG_EXT.1 External Audit Trail Storage

Testing Assurance Activities:

Test 1: The evaluator shall test this function by configuring this capability, performing auditable events, and verifying that the local audit storage and external audit storage contain identical data.

Test 2: The evaluator shall also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage.

Similar to the testing for FAU_GEN.1, this testing can be done in conjunction with the exercise of other functionality.

Test 3: Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one.

Test 4: If the TOE cannot perform audit reconciliation, then the TSS and the Guidance must explicitly state that there may be a gap in the audit server audit record if the connection between the audit server and ESM product is broken. The TSS must provide a characterization of that loss; further, the Guidance must provide instructions to the administrator on how to configure the ESM product to minimize the loss (e.g., increase local buffer size, inform the administrator of the loss of the connection, etc.). Lastly, the described loss minimization mechanisms must be tested to ensure that they behave as documented.

TD0066 was applied. (https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0066)

Testing Implementation Details/Results:

Test 1: The evaluator followed the procedures outlined in CC GUIDE Chapter 3 which describes configuration of TOE audit functionality. The evaluator observed audit entries in the Web GUI being captured in detail in a log file prior to transmission to the external audit server, then noted those same entries being present (with additional details provided per entry) in the audit log on the external audit server.

Test 1) result: PASS

Test 2: Not applicable, as the security target does not claim that the TOE perform a full consolidation of its local audit repository with an external audit server. The evaluator noticed that the PCE component of the TOE has a long buffering capability that allows multiple hours of generated audit events to be captured and forwarded onto the external syslog server when the network connection is re-established.

Test 2) result: PASS

Test 3: The evaluator used Wireshark to capture traffic for the case when the syslog-ng was stopped, then restarted to allow for traffic to be received from the PCE component of the TOE, this was successful, and all the audit events traffic was encrypted by the PCE. The Wireshark pcap files, and log entries on both sides showed the success of the communication.

Test 3) result: PASS

Test 4: The evaluator disconnected the syslog VM from the testing environment, generated audit events by running some TOE's management functions and verified that no audit events appeared in the offline syslog repository. After more than 6 hours of unavailability, the evaluator noticed that the PCE started enumerating the number of queued log messages and after a few more hours it displayed, in the web console, the number of lost log messages to be forwarded to syslog remote destinations.

Test 4) result: PASS

2.3.3 Identification and Authentication (FIA)

2.3.3.1 FIA_AFL.1 Authentication Failure Handling

Testing Assurance Activities:

Test 1: The evaluator shall test this capability by using the authentication function of the TSF to deliberately enter incorrect credentials. The evaluator shall observe that the proper action occurs after a sufficient number of incorrect authentication attempts.

Test 2: The evaluator shall also use the TSF to reconfigure the threshold value in a manner consistent with operational guidance to verify that it can be changed.

Testing Implementation Details/Results:

Test 1: The evaluator deliberately triggered a lockout with a local account, used the correct credentials and observed them being rejected for the entire lockout period, and was then able to login successfully after the lockout period ended.

Test 1) result: PASS

Test 2: The evaluator configured a different threshold to verify the unsuccessful authentication mechanism and a different lockout period and confirmed that the TOE behaved according to the new settings.

Test 2) result: PASS

2.3.3.2 FIA_SOS.1 Verification of Secrets

Testing Assurance Activities:

The evaluator shall test this capability in the following manner:

Test 1

a) *If password-based authentication is supported, the evaluator shall supply valid and invalid passwords in order to verify that the length and composition requirements function as described in the TSS.*

b) *The evaluator shall test the password aging requirements by setting a password and observing that it expires after the appropriate length of time.*

c) *The evaluator shall test reuse requirements by providing a series of valid and invalid changed passwords, first to test that a changed password must be sufficiently distinct and then to test that passwords cannot be reused within a certain number.*

Test 2 If password-based authentication is supported, the evaluator shall perform the steps described in the operational guidance to alter each configurable parameter of the password policy and to supply passwords before and after the parameter is altered to verify that the change appropriately took effect.

Test 3 If non-password-based authentication is supported, the evaluator shall follow the steps described in the operational guidance to create a credential. The evaluator shall then observe that providing that credential to the TOE allows access and an invalid credential is rejected.

An example of this is fingerprint biometrics. In this case, the evaluator would associate a user account with their own fingerprint. They would then log on to their account by providing their fingerprint and then observe failure when someone else tries to provide their fingerprint instead.

Testing Implementation Details/Results:

Test 1:

a) The evaluator conducted both positive and negative tests to confirm that the TOE support the password length of 16 and composition requirements stated in the ST.

b) The evaluator tested password aging by setting the maximum possible lifespan for a password, setting the time for the host system of the PCE component of the TOE beyond that lifespan, then observing that the password had expired.

c) The evaluator tested the password reuse capabilities by keeping track of previously used passwords, then checking the history capability by attempting to reuse a previously used password. The evaluator confirmed that the TOE behaved as expected with regards to the password reuse capability.

Test 1) result: PASS

Test 2: The evaluator tested the changing of parameters with password created before and after the parameter changed and by attempting to use a password previously acceptable when it no longer is.

Test 2) result: PASS

Test 3: The evaluator addressed this by attempting to pair a VEN with first an invalid key then a valid key.

The valid key was generated by the PCE pairing process, then altered to create the invalid key. *The evaluator observed that providing a valid pairing key to the VEN allows it to complete the pairing operation and providing an invalid pairing key fails the pairing operation, therefore this assurance activity is satisfied.*

Test 3) result: PASS

2.3.3.3 FIA_USB.1 User-Subject Binding

Testing Assurance Activities:

Test 1 The evaluator shall test this capability by configuring the TSF to accept user information from external sources as defined by the ST.

Test 2 The evaluator shall then perform authentication activities using these methods and validate that authentication is successful in each instance.

Test 3 Based on the defined privileges assigned to each of the subjects, the evaluator shall then perform various management tests in order to determine that the user authorizations are consistent with their externally defined attributes and the configuration of the TSF's access control policy.

For example, if a user who is defined in an LDAP repository belongs to a certain group and the TSF is configured such that members of that group only have read-only access to policy information, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF that they do not have write access to policy information. This verifies that the aspects of the user's identity data that are pertinent to how the TSF treats the user are appropriately taken from external sources and used in order to determine what the user is able to do.

Testing Implementation Details/Results:

Test 1: For the SAML-supported external authentication method, the evaluator made sure that the user permissions were consistent with those assigned to direct login credentials for users from each provider (SAML and PCE).

Test 1) result: PASS

Test 2: The evaluator was able to successfully login with the same role using PCE credentials and SAML credentials that were assigned that role.

Test 2) result: PASS

Test 3: The evaluator was able to perform actions, using PCE and SAML credentials, that were consistent. with the role assigned to each identity. The PCE component of the TOE, once integrated with the external SAML provider, assigns roles to identities from the external SAML. The evaluator also confirmed that when external SAML users were assigned different User-roles, these users behaved according to their assigned roles.

Test 3) result: PASS

2.3.4 Security Management (FMT)

2.3.4.1 FMT_MTD.1 Management of TSF Data

2.3.4.1.1 Testing Assurance Activities

Testing Assurance Activities:

Test 1 The evaluator shall test this capability by performing the identified management activities with authorized roles in order to determine that they are allowed.

Test 2 The evaluator shall also attempt to perform these activities with unauthorized roles in order to determine that they are not allowed.

Test 3 Finally, the evaluator shall verify that communications between the TSF and the authentication data repository are secured by repeating the testing for FTP_ITC.1 over the interface between the two components.

Testing Implementation Details/Results:

Test 1: The evaluator logged in to the PCE using a Global organization owner account and was able to create and delete Global administrator users. According to the ST, only the Global Organization owner account should be able to deleted user accounts, therefore, the evaluator determined that the TOE behaved as expected.

Test 1) result: PASS

Test 2: The evaluator logged in to the PCE console with Global administrator and was not able to see the local or external users, since the GUI only displays/allows the tasks designated for that role; the negative testing for activities not defined for a role cannot be exercised and this requirement is therefore satisfied *Test 3:* The evaluator addressed this by performing a Wireshark capture of a login with a SAML-provided identity and a separate capture of a login with a PCE-provided identity. Subsequent analysis of the pcap showed that the interactions between.

- The PCE and the web browser
- The web browser and the ADFS server

were all protected by TLS.

Using the SAML server as an ID provider showed no communication between the SAML server and the PCE server, and this is the correct and expected behavior.

Test 3) result: PASS

2.3.4.2 FMT_MOF.1 Management of Function Behavior

2.3.4.2.1 Testing Assurance Activities

Testing Assurance Activities:

Test 1 The evaluator shall test this function by accessing the TSF using one or more appropriately privileged administrative accounts and determining that the management functions as described in the ST and operational guidance can be managed in a manner that is consistent with any instructions provided in the operational guidance.

Test 2 If the TSF can be configured by an authorized and compatible Secure Configuration Management product, the evaluator shall also configure such a product to manage the TSF and use this product to perform the defined management activities.

Test 3 In addition, any access restrictions to this behavior should be enforced in a manner that is consistent with the relevant documentation. The evaluator shall test this by attempting to perform a sampling of the available management functions using one or more unprivileged accounts to observe that the activities are rejected or unavailable.

Testing Implementation Details/Results:

Test 1: Throughout testing, the evaluator performed a subset of management functions as a Global Administrator (with full system access) and as an Operator (with Global Viewer access) and observed that the TOE reacted in a consistent manner as described by the operational guidance. Users were able to perform the activities as per their designated roles Negative tests for attempting commands not available to a specific role could not be carried out as the Web GUI only displays commands permitted for that role, therefore the evaluator observed that the TOE behaved as expected

Test 1) result: PASS

Test 2: This is not applicable.

Test 2) result: PASS

Test 3: in this test case, the evaluator accessed the TOE using unprivileged account, and noticed that the privileged management functions were not available, which is the expected behavior.

Test 3) result: PASS

2.3.4.3 FMT_MOF_EXT.1 External Management of Functions Behavior

2.3.4.3.1 Testing Assurance Activities

Testing Assurance Activities:

Test 1 The evaluator shall test this capability by deploying the TOE in an environment where there is an Access Control component that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the Policy Management product to modify the behavior of the functions specified in the requirement above. For each function, the evaluator shall verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification.

Test 2 The evaluator shall also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities:

- ➢ *Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function's behavior and observe that the audit repository now logs (or doesn't log) this event based on the modified behavior.*
- *Repository for audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository.*
- *Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP such that that action is now disallowed (or allowed), perform the same action, and observe that the authorization differs from the original iteration of the SFP.*
- *Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the FSP.*
- *Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied.*

Test 3 Once this has been done, the evaluator shall reconfigure the TOE so that it is no longer authorized to manage the Access Control product. The evaluator shall then attempt to perform management functions using the TOE and observe that this is either disallowed or that the option is not even present.

Testing Implementation Details/Results:

Test 1: The evaluator addressed this by first installing the two instances of VEN: one on a laptop and another on a VM, each running Windows 10 enterprise edition. The evaluator then paired the VENs with PCE to create managed Workloads.

- *For Access Control SFP: The evaluator configured the testing environment such that the PCE is authorized to provision and install rulesets to the VEN. The evaluator used the PCE's SF to modify the rule policies for different IP sources and destination, for different protocols and services. For each rule policy, the evaluator set the rule that will allow some protocols or services and observed that the VEN appropriately enforced the rule, then the evaluator deleted or disabled the rule and observed that is the VEN disallowed the network traffic or service.*

Test 1) result: PASS

Test 2:

- *Audited events*: The Evaluator configured the VENs to only log allowed and blocked event traffic and noticed that the TOE behaved as expected, then the evaluator configured the VENs to only log Blocked traffic and noticed that the TOE behaved as expected and did not display any allowed traffic, then the evaluator turned off the visibility mode, and generated some network traffic. The evaluator waited for some time and observed non new network traffic displayed. The evaluator determined that the TOE behaved as expected.
- *Repository for audit storage: Not applicable, because the VEN only sends audit events to the PCE that it is paired with.*
- *Access Control SFP: the evaluator configured a policy that prevented one VEN from pinging the other, then the evaluator tried to ping the VEN and determined that the pings failed. The evaluator then changed the policy to permit the ping, then the 1st VEN was successful in pinging the 2nd VEN. The evaluator observed that the VEN behaved differently depending to policy rule configured in the PCE.*
- *Policy being implemented by the TSF: this was addressed in the test for the Access Control SFP.*
- *Not Applicable as the TOE does not have specific behavior to implement in the event of communications outage. In the case of a communication outage with the PCE, the VEN continue to enforce the current installed policy.*

Test 2) result: PASS

Test 3: The evaluator unpaired a VEN via the Web GUI, then deleted the VEN installation on the workload that had hosted the VEN. The act of unpairing resulted in the PCE no longer being able to 'see' the VEN, and thus there was no way for the PCE to issue an updated security policy to a VEN. The evaluator determined that providing a valid pairing key to the TOE allows pairing of the VEN to the PCE and providing an invalid pairing key was rejected by the PCE. The TOE behaved as expected.

Test 3) result: PASS

2.3.4.4 FMT_MSA_EXT.5 Consistent Security Attributes

2.3.4.4.1 Testing Assurance Activities

Testing Assurance Activities:

Test 1 The evaluator shall test this capability by defining policies that contain the contradictions indicated in the operational guidance and observing if the TSF responds by detecting the contradictions and reacting in the manner prescribed in the ST.

If the TSF behaves in a manner that prevents contradictions from occurring, the evaluator shall review the operational guidance in order to determine if the mechanism for preventing contradictions is described and if this feature is communicated to administrators.

This feature shall be tested in conjunction with a compatible Access Control product; in other words, if the TOE has a mechanism that prevents contradictions (for example, if a deny rule always supersedes an allow rule), then correct enforcement of such a policy by a compatible Access Control product is both a sufficient and a necessary condition for demonstrating the effectiveness of this mechanism.

Testing Implementation Details/Results:

Test 1: Not Applicable: Because the PCE employs an allow-list policy model, it is not possible for contradictory rules to be created. 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.

Test 1) result: PASS

2.3.4.5 FMT_SMF.1 Specification of Management Functions

2.3.4.5.1 Testing Assurance Activities

Testing Assurance Activities:

Test 1 The evaluator shall test this capability by accessing the TOE and verifying that all of the defined management functions exist, that they can be performed in the prescribed manner, and that they and accomplish the documented capability.

Testing Implementation Details/Results:

Test 1: The evaluator verified that all management functions exist and are accessible only by users with appropriate roles (i.e., Global administrators and Global Organization Owners). The TOE implements a Web-based management interface, as such access (or lack thereof) to management functions is based solely on the interface options presented to a logged-in user. Throughout the rest of the testing, individual management functions defined in the ST were exercised and the evaluator determined that they work in the prescribed manner. Since each management function listed in FMT_SMF.1 is tied to security functionality defined in other SFRs, and since all testing assurance activities for these SFRs were carried out, the evaluator concluded that this assurance activity is satisfied. The Test report, section 5.2.1, include a mapping table for the management functions.

Test 1) result: PASS

2.3.4.6 FMT_SMR.1 Security Management Roles

2.3.4.6.1 Testing Assurance Activities

Testing Assurance Activities:

Test 1 The evaluator shall test this capability by using the TOE in the manner prescribed by the operational guidance to associate different users with each of the available roles.

Test 2 If the TSF provides the capability to define additional roles, the evaluator shall create at least one new role and ensure that a user can be assigned to it.

Since other assurance activities for management requirements involve the evaluator assuming different roles on the TOE, it is possible that these testing activities will be addressed in the course of performing these other assurance activities.

Testing Implementation Details/Results:

Test 1: The evaluator addressed this with test 1 in section 2.3.4.2.1. The evaluator performed a subset of management functions as a Global Administrator (with full system access) and as a newly created operator (with Global Viewer access):

1. As Global Organization Owner, create new Global Administrator user
2. As Global Administrator user, try to find “Role-Based Access” menu (not present)
3. As Global Administrator user, change the state of a policy for a Workload.
4. As Global Organization Owner, change the Global Administrator user to Global Read Only
5. As the new Global Viewer user, try to change the state of the previously changed policy for the specific Workload (cannot edit)
6. As Global Organization Owner, delete the Global Viewer User

Test 1) result: PASS

Test 2: The TOE has predefined roles only and therefore this is not applicable.

Test 2) result: PASS

2.3.5 Protection of the TSF (FPT)

2.3.5.1 FPT_APW_EXT.1 Protection of Stored Credentials

2.3.5.1.1 Testing Assurance Activities

Testing Assurance Activities:

Test 1 The evaluator shall test this SFR by reviewing all the identified credential repositories to ensure that credentials are stored obscured, and that the repositories are not accessible to no administrative users.

Test 2 The evaluator shall similarly review all scripts and storage for mechanisms used to access systems in the operational environment to ensure that credentials are stored obscured, and that the system is configured such that data is inaccessible to non-administrative users.

Testing Implementation Details/Results:

Test 1 and Test 2: The evaluator verified that non-administrator users do not have access to the PCE database and that the database credentials are stored obscured in an encrypted file located in the PCE platform which is only accessible to the Illumio administrator. Also, the evaluator verified that non-administrator user could not access the folder of the file where the VEN keys are kept. SAML credentials used to access PCE are managed by an external provider of credentials, ADFS which is outside the scope of the evaluation.

Test 1) 2) results: PASS

2.3.5.2 FPT_SKP_EXT.1 Protection of Secret Key Parameters

2.3.5.2.1 Testing Assurance Activities

Testing Assurance Activities: None

Testing Implementation Details/Results: N/A

2.3.6 TOE Access (FTA)

2.3.6.1 FTA_SSL.3 TSF-initiated Termination

2.3.6.1.1 Testing Assurance Activities

Testing Assurance Activities:

Test 1 The evaluator shall test this capability by following the operational guidance to configure several different values for the inactivity time period referenced in the component; these shall consist at least of the minimum and maximum allowed values as specified in the operational guidance, as well as one other value. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.

Testing Implementation Details/Results:

Test 1: The evaluator configured two different timeout periods sequentially; and with sequential login sessions confirmed that the timeout worked correctly.

The evaluator configured the timeout to the minimum and maximum allowed values and observed that it worked correctly for both local users and SAML external users.

Test 1) result: PASS

2.3.6.2 FTA_SSL.4 User-initiated Termination

2.3.6.2.1 Testing Assurance Activities

Testing Assurance Activities:

Test 1 The evaluator shall test this [User-initiated termination] capability by establishing a session with the TOE using an administrative interface. The evaluator then follows the operational guidance to exit or log off of the session and observes that the session has been terminated. If applicable, the evaluator shall repeat this test for each administrative interface that is supported by the TOE.

Testing Implementation Details/Results:

Test 1: The evaluator observed with Wireshark that a remote session was terminated, confirmed that no further administrative actions were possible without re-authentication.

Test 1) result: PASS

2.3.6.3 FTA_TAB.1 TOE Access Banner

2.3.6.3.1 Testing Assurance Activities

Testing Assurance Activities:

Test 1 If the banner is not displayed by default, the evaluator shall configure the TOE in accordance with the operational guidance in order to enable its display. The evaluator shall then attempt to access the TOE and verify that a TOE banner exists.

Test 2 If applicable, the evaluator will also attempt to use the functionality to modify the TOE access banner as per the standards defined in FMT_SMF.1 and verify that the TOE access banner is appropriately updated.

Testing Implementation Details/Results:

Test 1: As the banner is not configured by default, the evaluator followed the guidance documents and configured the TOE to enable its display. Then the evaluator accessed the TOE and verified that the TOE correctly displayed the banner.

Test 1) result: PASS

Test 2: The evaluator changed the banner using TOE's guidance and confirmed the banner change with another login.

Test 2) result: PASS

2.3.7 Trusted Path/Channels (FTP)

2.3.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

2.3.7.1.1 Testing Assurance Activities

Testing Assurance Activities:

Test 1 The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

Test 2 For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE or the authorized IT entities.

Test 3 The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.

Test 4 The evaluators shall ensure that, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted[HD1] [MS2] . The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected.

Note: TD0576 https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0576 was applied to this AA.

Testing Implementation Details/Results:

Test 1: Communication was tested by running Wireshark to capture a new connection between the PCE and the external audit server, by shutting syslog-ng down, starting Wireshark, then performing a task via the Web GUI that results in the PCE generating an audit event that gets sent to the external audit server. The resulting PCAP showed the negotiation of the TLS session and sending of the audit event.

Test 1) result: PASS

Test 2: This was addressed by Test 1. The evaluator noticed that the TOE successfully initiated the communication channel with the audit server.

Test 2) result: PASS

Test 3: This was addressed by Test 1

Test 3) result: PASS

Test 4: This was addressed by unplugging the host system for PCE from the network, doing multiple actions over a period of time, plugging the PCE host system back in, and observing that the audit events generated during time the PCE was unplugged, have in fact been transferred securely to the external audit server.

Test 4) result: PASS

2.3.7.2 FTP_TRP.1 Trusted Path

2.3.7.2.1 Testing Assurance Activities

Testing Assurance Activities:

The evaluator shall perform the following set of tests and where applicable, repeat for each remote administration method:

Test 1 The evaluator shall ensure that communications using each protocol with each authorized IT entity, including each remote administration method, is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

Test 2 For communications using each protocol with each authorized IT entity and method of remote administration supported, the evaluator shall follow the guidance documentation to ensure that there is no available interface that can be used by a remote user to establish a remote administrative session without invoking the trusted path.

Test 3 The evaluator shall ensure that for communications of each protocol with each authorized IT entity, and for each method of remote administration, the channel data is not sent in plaintext.

Test 4 The evaluators shall ensure that, for each protocol and remote administration method combination tested during Test 1, the connection is physically interrupted. The evaluator shall then ensure that when physical connectivity is restored, communications are appropriately protected.

Note: TD0576 https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0576 was applied to this AA.

Testing Implementation Details/Results:

Test 1: The evaluator ran Wireshark to capture a new login session between a web browser and the PCE's Web GUI. The resulting PCAP showed the negotiation of the TLS session and successful login via the Web GUI. A negative test was run with the web browser trying to access the TOE through unsupported interface and noticed that the TOE rejected the https request.

Test 1) result: PASS

Test 2: this was addressed by Test 1 (only the Web GUI can be used)

Test 2) result: PASS

Test 3: this was addressed by Test 1

Test 3) result: PASS

Test 4: this was addressed by the evaluator using Wireshark to capture traffic during a logged-in session with the PCE, where administrative actions were performed and network connectivity with the VM running the web browser was dropped. The visual evidence proved that the session was restored, and the Wireshark captured showed that the session was always protected with TLS.

Test 4) result: PASS

3. Security Assurance requirements evaluation Activities (SARs)

3.1.1 ADV_FSP.1 Basic Functional Specification

Note: There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described for each SFR, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided. For example, if the TOE provides the capability to configure the key length for the encryption algorithm but fails to specify an interface to perform this function, then the assurance activity associated with FMT_SMF would fail.

3.1.1.1 TSS Assurance Activities

TSS Assurance Activities: None
TSS Implementation Details/Results: None

3.1.1.2 Evidence Assurance Activities

Evidence Assurance Activities: *The evaluator shall verify that the TOE functional specification describes the set of interfaces the TOE intercepts or works with. The evaluator shall examine the description of these interfaces and verify that they include a satisfactory description of their invocation.*
Evidence Assurance Activities Details/Results: The evaluator found the Security Target describes the Functional Specification sufficiently. The description of the interfaces, and how they are invoked, as provided in the ST is sufficient for the meet the requirements in ESM PM PP.

3.1.1.3 Testing Assurance Activities

Testing Assurance Activities: None
Testing Assurance Activities Details/Results: N/A

3.1.2 AGD_OPE.1 Operational User Guidance

3.1.2.1 TSS Assurance Activities

TSS Assurance Activities: None
TSS Implementation Details/Results: N/A

3.1.2.2 Guidance Assurance Activities

Guidance Assurance Activities:

Some of the contents of the operational guidance will be verified by the assurance activities with each SFR. The following additional information is also required.

The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

Guidance Assurance Activities Details/Results:

In reviewing the ST, the evaluator noted that Section 7.7 of the ST explicitly states that the TOE relies on the Operational Environment for all cryptographic operations used by the TOE. Further to this, CC GUIDE, Chapter 2, Section “Enable PCE FIPS Compliance”, details steps for configuring the RHEL cryptographic module on the PCE to FIPS mode, and chapter 6, Section “Enable FIPS Compliance for Windows VENs” includes same instructions for the VEN.

3.1.2.3 Testing Assurance Activities

Testing Assurance Activities: None

Testing Assurance Activities Details/Results: N/A

3.1.3 2.9.3 AGD_PRE.1 Preparative Procedures

3.1.3.1 TSS Assurance Activities

TSS Assurance Activities: None

TSS Implementation Details/Results: N/A

3.1.3.2 Guidance Assurance Activities

Guidance Assurance Activities:

As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms (that is, combination of hardware and operating system) claimed for the TOE in the ST.

Guidance Assurance Activities Details/Results:

The evaluator has determined that the combination of User Guidance documents listed in Section 1.1 adequately address all platforms claimed for the TOE in the ST.

The ST section 1.3 identifies the TOE as a software application. The TOE software is delivered as an rpm file, identified in chapter 2, section “install the PCE as an SNC of CC GUIDE.

The ST Section 3.2.2 specifies that the PCE component of the TOE will run on any platform that supports RHEL 8.2, but also provides some recommended hardware requirements in Table 3-4.

Accordingly, Table 3-3 of section 3.2.1 of the ST also identifies the Windows OS version that the VEN component of the TOE will run on.

The ST Section 1.2 Table 1-1 also identifies the minimum CPU requirements for the PCE and VEN components of the TOE.

3.1.3.3 Testing Assurance Activities

Testing Assurance Activities: None

Testing Assurance Activities Details/Results: N/A

3.1.4 ALC_CMC.1 Labeling of the TOE

3.1.4.1 TSS Assurance Activities

TSS Assurance Activities:

The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST.

TSS Implementation Details/Results:

Section 1.2 of the ST states that the TOE is the Illumio Core Platform v22.2.30.

3.1.4.2 Guidance Assurance Activities

Guidance Assurance Activities:

The evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

Guidance Assurance Activities Details/Results:

The evaluator has determined that the AGD guidance [CC guide] and TOE samples received for testing are consistent with the version number in the ST, and that this identifier is sufficient for an acquisition entity to use in procuring the TOE.

3.1.4.3 Testing Assurance Activities

Testing Assurance Activities: None

Testing Assurance Activities Details/Results: N/A

3.1.5 2.9.5 ALC_CMS.1 TOE CM Coverage

3.1.5.1 TSS Assurance Activities

TSS Assurance Activities: *The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements.*
TSS Implementation Details/Results: Section 1.2 of the ST states that the TOE is the Illumio Core Platform v22.2.30.

3.1.5.2 Guidance Assurance Activities

Guidance Assurance Activities: *By ensuring that the TOE is specifically identified, and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.*
Guidance Assurance Activities Details/Results: The evaluator confirms that the chapter 2, section "install the PCE as an SNC of CC GUIDE" also identifies the TOE as the version and build number from part of the name of the rpm installer.

3.1.5.3 Testing Assurance Activities

Testing Assurance Activities: None
Testing Assurance Activities Details/Results: N/A

3.1.6 ATE_IND.1 Independent Testing - Conformance

3.1.6.1 TSS Assurance Activities

TSS Assurance Activities: None
TSS Implementation Details/Results: N/A

3.1.6.2 Guidance Assurance Activities

Guidance Assurance Activities: None
Guidance Assurance Activities Details/Results: N/A

3.1.6.3 Testing Assurance Activities

Testing Assurance Activities:

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators shall document in the test plan that each applicable testing requirement in the ST is covered.

The Test Plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification shall address the differences between the tested platform and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale shall be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS/HTTPS, SSH). The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (that could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

Testing Assurance Activities Details/Results:

At the beginning of testing activities, the PCE was installed on a host platform with newly installed RHEL and was then put into the evaluated configuration. As part of the initial configuration, it was confirmed that both the PCE and the VENs have the appropriate software build and version. To install the PCE in the evaluated configuration the evaluator followed the steps described in the CC Guide.

The evaluator wrote an Evaluation Test Plan and executed it as formal testing. The following network diagram presents the test environment used by the evaluation team:

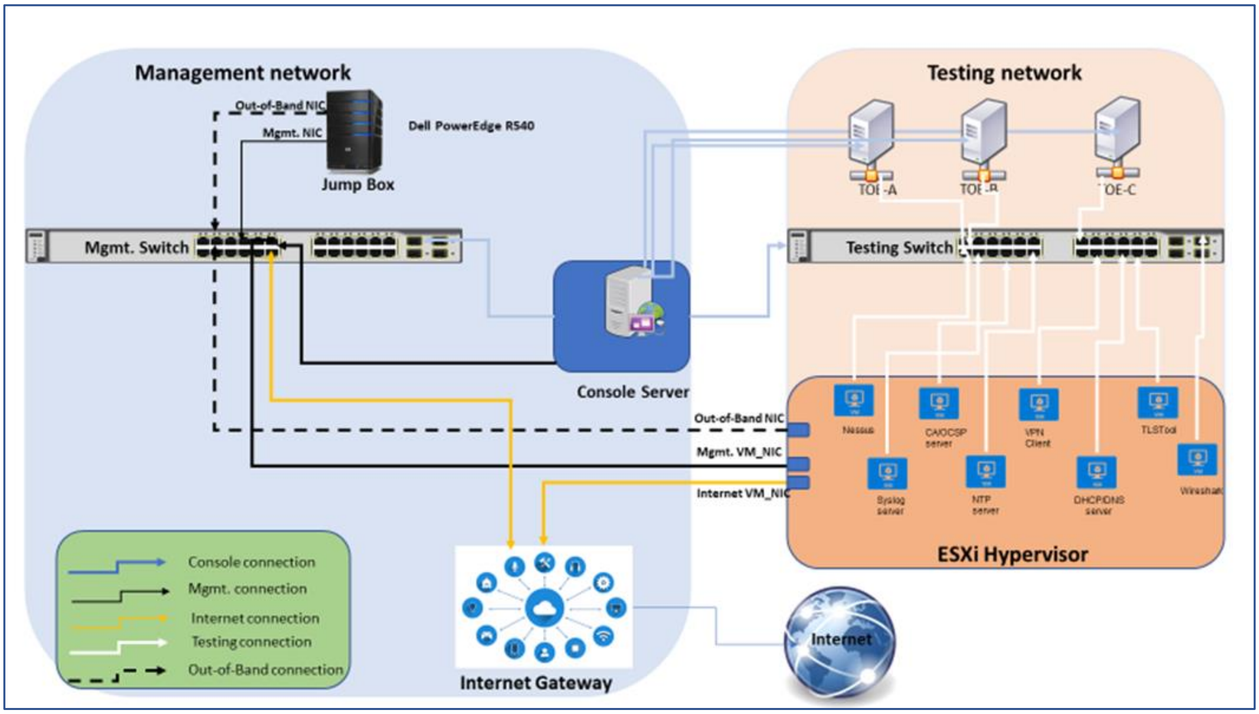

Figure 1: Network Topology

The following table details the supporting Platforms and Software using in the TOE operational environment.

Table 9:Testing Topology Details

Device	Devices information	Purpose
Tested platforms		
PCE	IPv4: 192.168.0.100 MAC: 2C:B8: ED: 33:8a:78 Host Name: PCE	TOE, connected to S1 port 1
VEN 1	IPv4: 192.168.0.101 MAC: 2C:B8: ED:21: A0:1a Host Name: VEN-1	TOE, connected to S1 port 2
Console Server	***BlackBox LES1608A***	***TOE's Console access***
Console server with USB and RJ45 interfaces	Console server with firewall integrated	Provide local console access to TOEs through USB or RJ45 interfaces
LAN switches		
S1	192.168.0.x/24	Switch with port mirroring capability
Virtualized servers		
Syslog Server	IPv4: 192.168.0.204 MAC: 00:0C:29: f5: E1:37 Host Name: syslog.lab.local	OS: Linux CentOS Stream v8 syslog-ng-3.35.1-1.el9.x86_64 Function: audit server
OpenSSL CA	IPv4: 192.168.0.208	OS: Linux CentOS Stream v8

OpenSSL OCSP Responder	MAC: 00:0C: 29:2F: 1E:6F Host Name: ca1.lab.local	Openssl version: OpenSSL 1.0.2k Function: CA and OCSP server
DNS and DHCP server	IPv4: 192.168.0.200 MAC: 00:0C:29:DB: 70:40 Hostname: ad.lab.local	OS: Windows Server 2016 Function: AD, DNS and DHCP servers
NTP Server	IPv4: 192.168.0.206 MAC: 00:0C: 29:5D: F7:E1 Hostname: ntp.lab.local	OS: Linux CentOS Stream v8 NTP version: 4.2.6p5 Function: ntp server
Wireshark VM	SPAN	OS: Linux CentOS Stream v8 Tools/version: Wireshark 2.6.2 (64 bits) Function: Network Traffic Monitor
VEN 2	IPv4: 192.168.0.102 MAC: 2C:B8: ED:24: A0:1a Host Name: VEN-2	Another VEN needed for testing
Management Host (PCE)	IPv4: 192.168.0.162 MAC: 00:0C:29: E4:37: B9 Hostname: mgmt.-1.lab.local	Linux CentOS Stream v8 Bitvise 6.47 and 8.35, putty 0.74, Zennmap v7.93, OpenVAS 22.4.0, Winscp v5.15.2
Management Host (VEN)	IPv4: 192.168.0.157 MAC: 00:0C: 29:CA:81:7B Hostname: mgmt.-2.lab.local	Windows 10 Enterprise Bitvise 6.47 and 8.35, putty 0.74, Zennmap v7.93, Winscp v5.15.2
Kali Linux	IPv4: 192.168.0.55 MAC: 00:0C:29: A8:3B:2D Hostname: OpenVAS.lab.local	OS: Windows 10 Enterprise Tools version: OpenVAS Pro version 21.4.3

The Test Report was supplied as part of the testing efforts. During testing activity, the TOE platform was installed in an isolated LAN, communicating with a setup of servers, installed in VMware ESXi server version 7.0.3. The Test Plan contains the platforms tested and documents all test cases dictated by the ESM PM PP. the test plan also contains initial configuration tests cases, manual tests, and penetration tests case. Each test case was performed and assigned a pass verdict resulting in overall pass verdict for the testing effort.

3.1.7 AVA_VAN.1 Vulnerability Survey

3.1.7.1 TSS Assurance Activities

Testing Assurance Activities: None

Testing Assurance Activities Details/Results: N/A

3.1.7.2 Guidance Assurance Activities

Guidance Assurance Activities: None

Guidance Assurance Activities Details/Results: N/A

3.1.7.3 Testing Assurance Activities

Testing Assurance Activities:

As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in this category of ESM application in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated.

Evaluation Activities Details/Results:

The complete vulnerability analysis is documented in the ETR and in the following reports:

- Illumio Core v22.2 Third-Party Libraries Vulnerability Analysis Report v0.5 Feb 4 2023.xlsx
- Illumio Core v22.2 Third-Party Libraries Vulnerability Analysis Report v0.4 Dec 19 2022.xlsx
- Illumio Core v22.2 Third-Party Libraries Vulnerability Analysis Report v0.3 Nov 03 2022.xlsx

The evaluator performed 3 CVE searches: on August 05, Dec 09-17, 2022, and Feb 04, 2023, with 585 search terms that included the TOE and all the internal components that compose the TOE. The search identified 171 results from which 64 were deemed as potentially applicable vulnerability.

When a CVE search produced a search result, the evaluator examined CVE details to determine if it is applicable to the TOE in the evaluated configuration. The following criteria were used:

a) if CVE is applicable to the relevant third-party library or simply contains a search string,

b) if vulnerability is applicable, if it is applicable to the version used in the TOE (i.e., check if it is already patched in the version used),

c) if it is clearly mitigated in the obvious manner (e.g., exploit requires shell access that is not offered by the TOE).

A pared-down list of remaining 64 matches then were sent to the vendor for further analysis. The vendor provided technical analysis and responded to the lab with additional details allowing to make final applicability determination.

The following search terms were utilized: Illumio, Linux kernel, intel Xeon E3 v6, intel Core i5-7500, Illumioos, TCP/IP, acpi, acpi-support-base, openssl, openjdk, acpid, adduser, at, base-files, base-passwd, busybox, bzip2, coreutils, cpio, cron, dash, debianutils, diffutils, dpkg, e2fslibs:amd64, e2fsprogs, ethtool, file, findutils, gcc-4.9-base:amd64, grep, gzip, hostname, ifupdown, inetutils-ping, init, init-system-helpers, initscripts, insserv, iproute2, kmod, less, libacl1:amd64, libapt-pkg4.12:amd64, libattr1:amd64, libaudit-common, libaudit1:amd64, libblkid1:amd64, libbz2-1.0:amd64, libc-bin, libc6:amd64, libcomerr2:amd64, libdb5.3:amd64, libdebconfclient0:am, libgcc1:amd64, libgdbm3:amd64, libkmod2:amd64, liblzma2, liblzma5:amd64, libmagic1:amd64, libmount1:amd64, libpam-modules:amd64, libpam-modules-bin, libpam-runtime, libpam0g:amd64, libpcre3:amd64, libperl4-corelibs-pe, libpng12-0:amd64, libpopt0:amd64, libprocps3:amd64, libselinux1:amd64, libsemanage-common, libsemanage1:amd64, libsepol1:amd64, libslang2:amd64, libsmartcols1:amd64, libss2:amd64, libstdc++6:amd64, libtinfo5:amd64, libusb-0.1-4:amd64, libustr-1.0-1:amd64, libuuid1:amd64, locales, login, logrotate, lsb-base, lsof, makedev, mawk, mksh, module-init-tools, mount, multiarch-support, ncurses-term, net-tools, netbase, passwd, patch, pdksh, perl, perl-base, perl-modules, procps, psmisc, readline-common, rsync, sed, startpar, strace, sysv-rc, sysvinit, sysvinit-core, sysvinitutils, tar, telnet, time, traceroute, tzdata, util-linux, vim-common, vim-tiny, xz-utils, 3ware Storage (RAID), Erlang OTP, Flask, Flask-RESTful, Jinja2, LZ4, MarkupSafe, PyMySQL, Werkzeug, aniso8601, apache-ant, apache-commons-beanutils, apache-commons-chain, apache-commons-codec, apache-commons-collections, apache-commons-dbcp, apache-commons-digester, apache-commons-discovery, apache-commons-el, apache-commons-fileupload, apache-commons-httpclient, apache-commons-httpcomponents, apache-commons-io, apache-commons-lang, apache-commons-logging, apache-commons-net, apache-commons-pool, apache-commons-validator, apache-log4j, apache-maven, apache-struts1, apache-taglib, apache-velocity, apache-xalan-j, apache-xerces, apache-xmlrpc, apr, apr-util, bash, busybox, cJSON, cabextract, click, crash, curl, cyrus-sasl, dhcpcd, dialog, dmidecode, e2fsprogs, eventlog, gdb, geoView, ghostscript, glib, googletest, grub, gsoap, haveged, heimdal, hibernate-validator, httpd, icu, image4j, iniparser, iptables, itsdangerous, jackson, javamail, jersey, jetty, jfreechart, json-cpp, jsoup, junit, kexec-tools, legacy-spidermonkey, libcups, libdnet, libesmtp, libevent, libgd, libmaxminddb, libmnl, libnftnl, libntlm, libpcap, libssh2, libxml2, libxslt, log4shib, mDNSResponder, mariadb-connector-c, mariadb-java-client, ncurses, net-snmp, nghttp2, nginx, node.js, ntp, open-vm-tools, opencsv, openldap, opensaml, openssh, openssl, pciutils, pcre, pycrypto, python-dateutil, python-magic, pytz, readline, requests, rng-tools, samba, semver, six, slf4j, spidermonkey, stunnel, syslog-ng, tcpdump, uWSGI, valgrind, virtualbox, vlan, xerces-c, xmlsecurity, xmltooling, xz, zlib.

The evaluator searched the following public vulnerability repositories:

- The National Vulnerability Database at https://nvd.nist.gov/vuln
- The CVE Details website at https://www.cvedetails.com/vulnerability-search.php

Both sites were checked using the search terms listed above, package name and version provided in the list, as in many instances, one website would yield one or more results while the other provided no results, and vice versa. In many instances, several potential vulnerabilities had to be checked for applicability. In every instance where each website generated hits, the results were cross checked for duplicate entries.

This list was cross-checked for completeness with the results of automated scanners (e.g., NMAP, OpenVas) and TOE's self-reporting capabilities. Based on the module and component list, the evaluator conducted a vulnerability search using publicly available sources to identify potential vulnerabilities. The identified potential vulnerabilities were communicated to the vendor for further analysis and mitigation.

The evaluator examined the TOE architecture and noted that it utilizes a database to store user data. The evaluator theorized that it is possible the TOE would be vulnerable to SQL injection attacks through the main web-based administrative interface. The evaluator devised a set of penetration tests targeting SQL injection to the specific version of database. The evaluator was unsuccessful in carrying out SQL injections as documented in the ETR AVA_VAN.1.

The evaluator identified potential vulnerabilities and provided systematic recommendations to mitigate them. The vendor provided a detailed explanation as to why the vulnerability did not apply to the TOE. A combination of scanning and vendor affirmation and reasoning enabled the evaluator to verify that the evaluated product is free from any vulnerabilities identified during the evaluation process.

The evaluator has confirmed that all identified vulnerabilities were either remediated, considered inapplicable, or deemed unfeasible, indicating that no residual vulnerabilities are present in the product. Consequently, further analysis of attack potential was deemed unnecessary.