National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Illumio Core v22.2.30

Report Number: CCEVS-VR-VID11335-2023

Version: 0.3

Dated: March 3, 2023

National Institute of Standards and Technology

Information Technology Laboratory

100 Bureau Drive

Gaithersburg, MD 20899

Department of Defense

ATTN: NIAP, SUITE 6982

9800 Savage Road

Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin
Jerome Myers
Meredith Martinez
DeRon Graves

The Aerospace Corporation

Common Criteria Testing Laboratory

Fathi Nasraoui

Nithya Rachamadugu

DEKRA Cybersecurity Certification Laboratory,

Sterling, Virginia, USA

Table of Contents

Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Illumio Core v22.2.30, provided by Illumio. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the DEKRA Cybersecurity Certification Common Criteria Testing Laboratory (CCTL) in Sterling, Virginia, United States of America, and was completed in March 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by DEKRA. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the *Standard Protection Profile for Enterprise Security Management-Policy Management, version 2.1* [ESM_PM_PP].

The TOE, Illumio Core 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 Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5), as interpreted by the Assurance Activities contained in the [ESM_PM_PP].

This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the [ESM_PM_PP] Assurance Activities. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Illumio Core v22.2.30 Security Target, Version 0.6, March 01, 2023, and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities that are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance results of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Illumio Core v22.2.30
Protection Profile	Standard Protection Profile for Enterprise Security Management-Policy Management, version 2.1, October 24, 2013 (ESM_PM_PP)
Security Target	Illumio Core v22.2.30 Security Target, v0.6, March 01, 2023
Evaluation Technical Report	Evaluation Technical Report for Illumio Core v22.2.30 Volume 1: Evaluation of the ST, version 0.2, March 01, 2023 Evaluation Technical Report for Illumio Core v22.2.30 Volume 2: Evaluation of the TOE, version 0.7, March 01, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
Conformance Result	CC Part 2 extended; CC Part 3 conformant
Sponsor	Illumio

Developer	Illumio
Common Criteria Testing Lab (CCTL)	DEKRA Cybersecurity Certification, Sterling, Virginia, USA
CCEVS Validators	Daniel Faigin DeRon Graves Meredith Martinez Jerome Myers

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Introduction

The TOE, Illumio Core 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).

3.2 Physical Boundaries

The TOE is a software application that is installed on the operating system running on the server hardware. The PCE is delivered as an RPM package compatible with RHEL 8.2. The VEN is an MSI compatible with Windows Installer 5.0 that is compatible with Windows 10 Enterprise. All installers are secured with an end-user generated public key and downloaded from the vendor's secure support portal.

The TOE does not include the hardware or operating systems of the systems on which it is installed. It also does not include the third-party software that is required for the TOE to run.

The following table lists the TOE software components and the operating environment in the evaluated configuration.

Table 2: Host Platform Environment Components

TOE Component Definition	Operational Environment	
	Operating System	**CPU**
PCE- Policy Compute Engine	Red Hat Enterprise Linux 8.2	Intel Xeon Silver 4216
VEN- Virtual Enforcement Node	Windows 10 Enterprise	Intel Core i7-8665U with AES-NI

4 Security Policy

4.1 Enterprise Security Management

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

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

The TOE implements a whitelist access control policy model; consequently, the TOE does not allow

any contradictory policy to be defined.

The PCE generates policy that the VEN consumes and implements. When an administrator modifies or creates a security policy rule, the PCE generates an updated overall policy and calculates policy changes for each affected VEN as part of the process called provisioning. All paired VENs periodically connect to the PCE to check for policy updates. If the VEN cannot connect to the PCE, it continues to enforce the last-known-good policy. If the VEN fails to connect to PCE on two consecutive occasions (an outage approximately corresponding to 10 minutes), the VEN enters a degraded state.

4.2 Security Audit

The TOE generates audit records of security relevant events as they occur. Any use of a management functions via the Web UI, as well as relevant IT environment events, will be audited. The PCE uses the RHEL auditing daemon (rsyslog or syslog-ng) for storing local audit trail (e.g., in /var/log/), and is capable of uploading logs to an external audit server over a secure channel.

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

- Heartbeat events are reported every 5 minutes.
- Traffic flows are reported every 10 minutes.
- Changes to network interfaces are reported asynchronously.

The PCE generates audit events when the APIs are invoked.

4.3 Identification and Authentication

The TOE requires users to be identified and authenticated before they can access any of the TOE's functions. Users are locked out of their accounts when they fail to log in after consecutive failures.

The number of unsuccessful authentication attempts can be configured by changing the default value of the runtime variable in the configuration file.

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

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

4.4 Security Management

The PCE maintains the administrative user roles: Global Organization owner, Global Administrator, Global Viewer, Global Policy Object provisioner, Global Ruleset Provisioner and Full Ruleset Manager. Each of these roles has varying levels of privileges which determine what management functions the administrative users are able to perform via the TOE's Console interface which is a web-based GUI.

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

The TOE restricts management functions to the "Global Organization Owner" administrator role. An administrator will authenticate to the TOE by providing their local or domain user credentials.

4.5 Protection of the TOE Security Functions

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

4.6 TOE Access

The TOE can be configured by an administrator to force an interactive session's termination based on a timeout value. A remote session that is inactive for the defined timeout value will be terminated. Once terminated, the user will be required to re-enter their username and password in order to establish a new session. The TOE can be configured to display advisory banners as part of the authentication prompt.

4.7 Trusted Path/Channels

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

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

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

5 Assumptions, Threats, Objectives and Clarification of Scope

5.1 Assumptions

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

- A.CRYPTO: The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
- A.ESM: The TOE will be able to establish connectivity to other ESM products in

order to share security data.

- A.ROBUST: The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
- A.SYSTIME: The TOE will receive reliable time data from the Operational Environment.
- A.USERID: The TOE will receive identity data from the Operational Environment.
- A.MANAGE: There will be one or more competent individuals assigned to install, configure, and operate the TOE.

5.2 Threats

The following lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

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

5.3 Objectives

The following identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

- O.ACCESSID: The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.

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

5.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Standard Protection Profile for Enterprise Security Management-Policy Management, Version 2.1, October 24, 2013 (ESM_PM_PP)
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor serious attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Section 6 of the Security Target and their operation with respect to the TOE is described in Section 7 of the Security Target. Any other functionality provided by Illumio Core needs to be assessed separately and no further conclusions can be drawn about their effectiveness.
- The evaluated configuration of the TOE is the Illumio Core v22.2.30. software product

and not any earlier or later versions released or in process. The TOE includes all the code that enforces the policies identified (see Section 4).

- The TOE supports several features that are not part of the evaluated functionality. These features are not tested and excluded from the scope of the evaluation:
    - Use of the SMTP
    - High Availability and Failover functionality
    - JSON/REST API use
    - Policy-based encryption (SecureConnect)
    - Configuration of policy targeting unmanaged Workloads
    - LDAP Authentication
    - VEN running on Linux operating system.
    - All visual aspects of the visualization feature, also known under the term Illumination map (except the option of "adding rule" through the feature)
- The VEN (part of the TOE) runs on multiple OS platforms, however not all of them were tested, only the Windows Enterprise is part of the evaluated configuration.

6 Documentation

The vendor provides a standard set of guidance documents that covers the core functionality of the product. These documents were used during the evaluation of the TOE:

- Illumio Core v22.2.30 Common Criteria Guide, February 2023
- Illumio Core version 22.2 PCE Administration Guide, February 2023
- Illumio Core version 22.2.1 Security Policy Guide, June 2022
- Illumio Core version 22.2.1 VEN version 22.2.0 Administration Guide, June 2022

These guidance documents contain the security-related guidance material for this evaluation and must be referenced to place the product within the Common Criteria evaluated configuration. The guidance documents are applicable for the version of Illumio Core claimed by this evaluation.

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the Illumio Core v22.2.30 software installed upon a general-purpose server platform.

Section 3.2 describes the TOE's boundary as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to communicate with the following environmental components:

- Web Browser used for remote administration of the TOE.
- Database for storage of configuration, operation, and audit data for the TOE.
- Authentication Store provide enterprise authentication and user data.
- Underlying endpoint system for hosting the Illumio Core software.
- Underlying Server on which the Illumio Core software is installed.

To use the product in the evaluated configuration, the product must be configured as specified in the *Illumio Core v22.2.30 Common Criteria Guide, February 2023* document. Refer to Section 6 for the full list of documents needed for instructions on how to place the TOE in its evaluated configuration.

8 IT Product Testing

This section describes the testing efforts of the Evaluation Team. The information is derived from the *Illumio Core v22.2.30 Evaluator Test Report, Version 0.6, March 01, 2023* document. The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

8.1 Developer Testing

PP ESM_PM v2.1 October 2013 evaluations do not require developer testing evidence for assurance activities.

8.2 Evaluator Independent Testing

A test plan was developed in accordance with the Testing Assurance Activities specified in the PP_ESM_PM v2.1 October 2013

The formal testing activity was conducted between Nov 22, 2022 to Dec 05, 2022 with TOE installed in the DEKRA lab located at 405 Glenn Dr, Suite 12, Sterling, VA 20164.

The Evaluator successfully performed the following activities during independent testing:

- Placed TOE into evaluated configuration by following the preparative procedures.
- Successfully executed the ESM PM v2.1 Assurance-defined tests.
- Planned and executed a series of vulnerability/penetration tests.

It was determined after examining the Test Report and full set of test results provided by the evaluators the testing requirements for PP ESM PM v2.1 October 2013 are fulfilled.

8.3 Testing Topology

As shown below, the test topology is configured for a dedicated and fully isolated ‘Test’ LAN. This setup prevents general access while still granting evaluators direct access to the TOE. The setup consists of a ‘Test’ LAN for IPv4. The server is local to the ‘Test’ LAN and packet capture is done by a VM connected to a mirrored port on the switch. All devices in the testing setup are synchronized through an NTP server.

Note: The diagram below shows the components involved in the testing.

Figure 1: TOE Test Environment network diagram

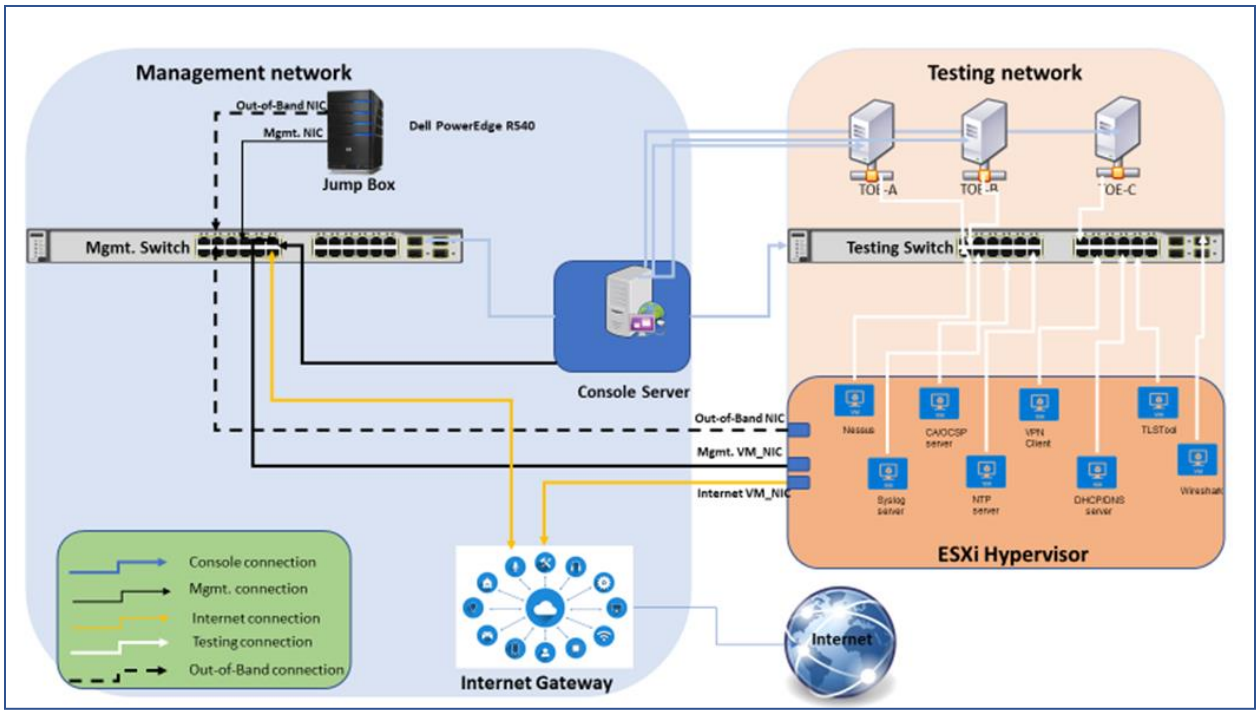

Table 3: Testing Topology Identifiers

Device	Devices information	Purpose
Tested platforms		
PCE	IPv4: 192.168.0.100 Host Name: PCE	TOE, connected to S1 port 1
VEN 1	IPv4: 192.168.0.101 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 Host Name: syslog.lab.local	OS: Linux CentOS Stream v8 syslog-ng-3.19.1-1.e17.x86_64 Function: audit server
OpenSSL CA OpenSSL OCSP Responder	IPv4: 192.168.0.208 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 Hostname: ad.lab.local	OS: Windows Server 2016 Function: AD, DNS and DHCP servers

Device	Devices information	Purpose
NTP Server	IPv4: 192.168.0.206 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 3.0.2 (64 bits) Function: Network Traffic Monitor
VEN 2	IPv4: 192.168.0.102 Host Name: VEN-2	Another VEN needed for testing
Management Host (PCE)	IPv4: 192.168.0.162 Hostname: mgmt.-1.lab.local	Linux CentOS Stream v8 Bitvise 6.47 and 8.35, putty 0.74, nmap 7.80, OpenVAS 22.4.0, Winscp v5.15.2
Management Host (VEN)	IPv4: 192.168.0.157 Hostname: mgmt.-2.lab.local	Windows 10 Enterprise Bitvise 6.47 and 8.35, putty 0.74, nmap 7.80, OpenVAS 22.4.0, Winscp v5.15.2
OpenVAS Scanner	IPv4: 192.168.0.215 Hostname: OpenVAS.lab.local	OS: Windows 10 Enterprise Tools version: OpenVAS Pro version 22.4.0

8.4 Test Hardware

The testing environment in the lab has been implemented using the following hardware:

- Dell N3024 Switch with port-mirroring capabilities.
- Dell PowerEdge R350 used as Jump Box Server to access the local testing environment: running Windows 10 Professional
- Dell PowerEdge R550 server running VMWare ESXi 7.0 update 3.
- Dell PowerEdge R440 running RHEL 8.2

8.5 Test Software

All testing was conducted using the following software:

- Wireshark v3.6 (64-bit)
- OpenVAS v8.13 with a full set of plugins
- Nmap v7.92
- Firefox 62.0 and Firefox 66.0
- DB Browser for SQLite 3.10.1 (64-bit)
- For Audit Server:
    - CentOS 8.2 with syslog-ng version 3.35.1
- For Active Directory Federated Services, Time Server, DNS Server:
    - Windows Server 2012 R2

- For remote management VM:
    - Windows 10 Professional

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluator determined the TOE to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Evaluation Activities specified in the [ESM_PM_PP].

The following evaluation results are extracted from the proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluator ensured the ST contained a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the [ESM_PM_PP] in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit specified in the [ESM_PM_PP]. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit specified in the [ESM_PM_PP]. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit specified in the [ESM_PM_PP], as well as the Assurance Activities specified for ALC_CMC.1 and ALC_CMS.1. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit specified in the [ESM_PM_PP]. The evaluation team ran the set of tests specified by the Assurance Activities in the ESM_PM_PP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the [ESM_PM_PP], and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit specified in the [ESM_PM_PP]. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The evaluator performed 3 CVE searches: on August 05, 2022, Dec September 17, 2022, and Feb 04, 2023, with 585 search terms that included the TOE and all the internal components that compose the TOE on 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

Additional detail on the search terms used and additional findings can be found in Section 3.1.7 of the AAR. The evaluator confirmed that all identified vulnerabilities were either remediated, considered inapplicable, or deemed unfeasible, indicating that no residual vulnerabilities are present in the product.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the [ESM_PM_PP], and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the [ESM_PM_PP], and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Illumio Core v22.2.30 Common Criteria Guide, February 2023* document. No versions of the TOE and software, either earlier or later were evaluated by NIAP.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

The excluded functionality is specified in section 5.4 of this report. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Security Target

The security target for this product's evaluation is Illumio Core v22.2.30 Security Target, v0.6, March 01, 2023.

12 Acronyms

Acronym	Definition
CC	Common Criteria
CM	Configuration Management
CSP	Critical Security Parameter
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IT	Information Technology
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
OSP	Organizational Security Policy
PM	Policy Management
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target

TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
ERP	Enterprise Resource Planning Applications

13 Terminology

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

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

14 Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] DEKRA Cybersecurity Certification CCTL (https://www.dekra.us/).

CCEVS Documents

[3] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5.

[4] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 5.

[5] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 5.

[6] Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.

Other Evaluation Documents

[7] Illumio Core v22.2.30 Security Target, v0.6, March 01, 2023

[8] Illumio Core version 22.2 PCE Administration Guide, February 2023

[9] Illumio Core version 22.2.1 Security Policy Guide, June 2022

[10] Illumio Core version 22.2.1 VEN version 22.2.0 VEN Administration Guide, June 2022

[11] Illumio Core v22.2.30 Common Criteria Guide, February 2023

[12] Assurance Activity Report for Illumio Core v22.2.30, version 0.7, March 01, 2023

[13] Evaluation Technical Report for Illumio Core v22.2.30 Volume 1: Evaluation of the ST, version 0.2, March 01, 2023

[14] Evaluation Technical Report for Illumio Core v22.2.30 Volume 2: Evaluation of the TOE, version 0.7, March 01, 2023

[15] Illumio Core v22.2.30 Evaluator Test Report, Version 0.6, March 01, 2023