National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Cisco Identity Services Engine (ISE) V3.1

Report Number: CCEVS-VR-VID11407-2023

Dated: September 27, 2023

Version: 0.2

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

Jerome Myers

The Aerospace Corporation

Richard (Rip) Toren

Anne Gugel

Farid Ahmed

Johns Hopkins University - Applied Physics Laboratory

Common Criteria Testing Laboratory

Halil Tosunoglu

Raj Mendon

Rupal Gupta

Shaunak Shah

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Identity Services Engine (ISE) V3.1 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in September 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both developed by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the U.S. Government collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e & Network Device collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0.

The TOE identified in this VR has been evaluated at a NIAP-approved CCTL 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 Protection Profile (PP). This VR 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 ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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 ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by NIAP approved commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (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 IT 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 Compliant 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 result of the evaluation.
- The Protection Profile(s) 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	Cisco Identity Services Engine (ISE) V3.1
Protection Profile	collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, March 23, 2020 & Network Device collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0, January 25, 2015.
Security Target	Cisco Identity Services Engine (ISE) V3.1 Security Target, Version 1.4
Evaluation Technical Report	Cisco Identity Services Engine (ISE) V3.1 Evaluation Technical Report, Version 0.3
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Jerome Myers Farid Ahmed

Item	Identifier
	Anne Gugel Richard Toren

3 Architectural Information

3.1 TOE Description

This section provides an overview of the Cisco Identity Services Engine (ISE) v3.1 TOE and a brief description of the capabilities of the ISE product. ISE is a consolidated policy-based access control system that combines authentication, authorization, accounting (AAA) and guest management in one appliance. ISE v3.1 software runs on the Cisco Application Deployment Engine (ADE) Release 3.1 operating system (ADE-OS). ADE-OS is a Cisco-proprietary Red Hat Enterprise Linux-based operating system [RHEL v8.2]

The TOE also includes an instance of the Embedded Services Router 5921 [ESR], running IOS 15.8(3)M7. The ESR is a software-only solution for routing capabilities. The ESR provides IPsec session capabilities for ISE v3.1 to secure the channel between the TOE and NAS. The IOS image, that includes the cryptographic module IOS Common Cryptographic Module (IC2M), runs as a process on the RHEL bundle included in the ADE-OS.

Network access has evolved beyond just simple user name and password verifications. Additional attributes related to users and their devices are used as decision criteria in determining authorized network access. Additionally, network service provisioning can be based on data such as the type of device accessing the network, including whether it is a corporate or personal device. Cisco ISE is a scalable solution that helps network administrators meet complex network access control demands by managing the many different operations that can place heavy loads on applications and servers, including:

- Authorization and authentication requests.
- Queries to identity stores such as Active Directory and LDAP databases.
- Device profiling and posture checking.
- Enforcement actions to remove devices from the network.
- Reporting

ISE delivers secure access control across wired, wireless, and VPN connections. ISE can reach deep into the network to deliver visibility into who and what are accessing resources. Through the device profiler feed service, ISE delivers automatic updates of Cisco's validated device profiles for various IP-enabled devices from multiple vendors which simplifies the task of keeping an up-to-date library of the newest IP enabled devices.

The Cisco Secure Network Server(SNS) is based on the Cisco UCS® C220 Rack Server and is configured specifically to support the Cisco ISE security application. The Secure Network Server supports these applications in five versions. The Cisco Secure Network Server 3615 is designed for small deployments. The Secure Network Servers 3595, 3655, and 3695 has several redundant components such as hard disks and power supplies, making it suitable for larger deployments that require highly reliable system configurations. The Secure Network Servers 3615, 3655, and 3695 are recommended for

new installations whereas the Secure Network Server 3595 is recommended for existing installations.

Apart from the SNS models described above, ISE is also available as a Virtual Machine running on ESXi 6.7/7.0 on UCSC-C220-M5SX. Cisco ISE supports other virtual environment platforms, but only the ESXi 6.7 and 7.0 environments are a part of the evaluated configuration.

3.2 Physical Scope of the TOE

The Cisco ISE software runs on the Cisco Application Deployment Engine (ADE) Release 3.1 operating system (ADE-OS). The Cisco ADE-OS and Cisco ISE software run on a dedicated Cisco ISE 3500/3600 Series appliances and on ESXi 6.7/7.0 running on Cisco UCS C220-M5SX (UCSC-C220-M5SX). All models include the same security functionality.

Table 2: TOE Models

Hardware Models	**Cisco Identity Services Engine Appliance 3595 (SNS-3595)**	**Cisco Identity Services Engine Appliance 3615 (SNS-3615)**	**Cisco Identity Services Engine Appliance 3655 (SNS-3655)**	**Cisco Identity Services Engine Appliance 3695 (SNS-3695)**	**Cisco Identity Services Engine – VM running on ESXi 6.7and 7.0/UCSC-C220-M5SX (ISE-VM)**
Processors	Intel Xeon E5-2640 v3 (Haswell)	Intel Xeon Silver 4110 (Skylake)	Intel Xeon Silver 4116 (Skylake)	Intel Xeon Silver 4116 (Skylake)	Intel Xeon Silver 4116 (Skylake)[1]
Memory	64 GB	32 GB	96 GB	256 GB	96 GB

[1] While tested on the Intel Xeon Silver 4116 (Skylake), any Intel Xeon Scalable processor with the Skylake-SP microarchitecture may be used as part of the evaluated configuration with VMware ESXi 6.7/7.0

Hardware Models	Cisco Identity Services Engine Appliance 3595 (SNS-3595)	Cisco Identity Services Engine Appliance 3615 (SNS-3615)	Cisco Identity Services Engine Appliance 3655 (SNS-3655)	Cisco Identity Services Engine Appliance 3695 (SNS-3695)	Cisco Identity Services Engine – VM running on ESXi 6.7and 7.0/UCSC-C220-M5SX (ISE-VM)
Hard disk	4x600Gb disk	1x600 Gb disk	4x600Gb disk	8x600Gb disk	4x600Gb disk
RAID	Yes (RAID 0+1)	No	Yes (RAID 1+0)	Yes (RAID 1+0)	Yes (RAID 1+0)
Expansion slots	- Two PCIe slots (on a riser card)	- Two PCIe slots (on a riser card)	- Two PCIe slots (on a riser card)	- Two PCIe slots (on a riser card)	- Two PCIe slots (on a riser card)
Serial port (RJ-45 Connector)	2	2	2	2	2
USB 2.0 ports	0	0	0	0	0
USB 3.0 ports	4	4	4	4	4
1-GB Ethernet	1	1	1	1	1

Hardware Models	Cisco Identity Services Engine Appliance 3595 (SNS-3595)	Cisco Identity Services Engine Appliance 3615 (SNS-3615)	Cisco Identity Services Engine Appliance 3655 (SNS-3655)	Cisco Identity Services Engine Appliance 3695 (SNS-3695)	Cisco Identity Services Engine – VM running on ESXi 6.7and 7.0/UCSC-C220-M5SX (ISE-VM)
Management Port					
Video ports	2	2	2	2	2
Hypervisor	None	None	None	None	ESXi 6.7/7.0

4 Security Policy

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Cryptographic Support
3. Communications
4. Identification and Authentication
5. Security management
6. Protection of the TSF
7. TOE Access
8. Trusted path/channels

These features are described in more detail in the subsections below.

4.1 Security Audit

The TOE's Audit security function supports audit record generation and review. The TOE provides date and time information that is used in audit timestamps. The events generated by the TOE include indication of the logging starting and stopping, cryptographic operations, attempts to log onto the TOE, all commands/ web-based actions executed by the Security Administrator, and other system events.

The TOE can store the generated audit data on itself and it can be configured to send syslog events to other devices, including other iterations of ISE, using a TLS protected collection method. Logs are classified into various predefined categories. The TOE also provides the capability for the administrator to customize the logging output by editing the categories with respect to their targets, severity level, etc. The logging categories help describe the content of the messages that they contain. Access to the logs is restricted only to the Security Administrator, who has no access to edit them, only to copy or delete (clear) them. Audit records are protected from unauthorized modifications and deletions.

The logs can be viewed by using the Operations -> Reports page on the ISE administration interface, then select the log from the left side and individual record (message). The log record includes the category name, the message class, the message code (type of event), the message text (including a date/time stamp, subject (user) associated with the event, outcome of the event, etc.) and the severity level associated with the message. The previous audit records are overwritten when the allocated space for these records reaches the threshold.

4.2 Cryptographic Support

The TOE provides cryptography support for secure communications and protection of information. The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; asymmetric key generation; cryptographic key establishment using RSA-based and ECDSA key establishment schemes and DH key establishment; digital signature using RSA and

ECDSA; cryptographic hashing using SHA1 (and other sizes); random bit generation using DRBG and keyed-hash message authentication using HMAC-SHA (multiple key sizes). ISE uses the CiscoSSL FIPS Object Module (FOM) Cryptographic Implementation as its cryptographic module. The TOE implements the secure protocols - SSH and TLS/HTTPS on the server side and TLS on the client side. The TOE provides IPsec session capabilities for ISE v3.1 to secure the channel between the TOE and NAS. The TOE leverages the IOS Common Cryptographic Module (IC2M) for IPsec capabilities. The algorithm certificate references are listed in the table below.

Table 3: CAVP Certificate References

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_CKM.1	RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	CiscoSSL FIPS Object Module (FOM) 7.2a	RSA FIPS PUB 186-4 Key Generation (2048-bit key, 4096-bit key)	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	RSA FIPS PUB 186-4 Key Generation (2048-bit key, 4096-bit key)	A1462
	ECC schemes using "NIST curves" [selection: P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	CiscoSSL FIPS Object Module (FOM) 7.2a	ECDSA Key Generation FIPS PUB 186-4, "Digital Signature Standard (DSS)" (256 bits, 384 bits and 521 bits) NIST curves- P-256, P-384 and P-521	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	ECDSA Key Generation FIPS PUB 186-4, "Digital Signature Standard (DSS)" (256 bits, 384 bits and 521 bits) NIST curves- P-256, P-384 and P-521	A1462

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1	CiscoSSL FIPS Object Module (FOM) 7.2a	DSA Key Generation FIPS PUB 186-4, "Digital Signature Standard (DSS)"	A1420 A2697
	FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]	N/A	N/A	Vendor Affirmed
FCS_CKM.2	RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"	N/A	N/A	Vendor Affirmed
	Elliptic curve-based key establishment schemes that meet the	CiscoSSL FIPS Object Module (FOM) 7.2a	CVL-KAS-ECC	A1420 A2697

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”	IOS Common Cryptographic Module (IC2M) Rel5a	CVL-KAS-ECC	A1462
	Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”	CiscoSSL FIPS Object Module (FOM) 7.2a	CVL-KAS-FFC	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	CVL-KAS-FFC	A1462
	FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [groups listed in RFC 3526]	N/A	N/A	Vendor Affirmed

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_COP.1/ DataEncryption	AES used in [CBC, CTR, GCM] mode and cryptographic key sizes [128 bits, 256 bits]	CiscoSSL FIPS Object Module (FOM) 7.2a	AES CBC (128 and 256 bits) CTR (128 and 256 bits) GCM (128, and 256 bits)	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	AES CBC (128 and 256 bits)	A1462
FCS_COP.1/ SigGen	For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	CiscoSSL FIPS Object Module (FOM) 7.2a	RSA FIPS PUB 186-4 Signature Generation & Verification (2048-bit key, 4096-bit key)	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	RSA FIPS PUB 186-4 Signature Generation & Verification (2048-bit key, 4096-bit key)	A1462
	For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256,	CiscoSSL FIPS Object Module (FOM) 7.2a	ECDSA FIPS PUB 186-4, "Digital Signature Standard (DSS)" (256 bits, 384 bits and 521 bits)	A1420 A2697

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	P-384, P-521]; ISO/IEC 14888-3, Section 6.4		NIST curves- P-256, P-384 and P-521	
		IOS Common Cryptographic Module (IC2M) Rel5a	ECDSA FIPS PUB 186-4, “Digital Signature Standard (DSS)” (256 bits, 384 bits and 521 bits) NIST curves- P-256, P-384 and P-521	A1462
FCS_COP.1/ Hash	[SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits	CiscoSSL FIPS Object Module (FOM) 7.2a	SHS (SHA-1, SHA-256, SHA-384, and SHA-512)	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	SHS (SHA-1, SHA-256, SHA-384, and SHA-512)	A1462
FCS_COP.1/ KeyedHash	[HMAC-SHA-1, HMAC-SHA- 256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [key size (in bits) used in HMAC] and message digest sizes [160, 256, 384, 512] bits	CiscoSSL FIPS Object Module (FOM) 7.2a	HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA384, and HMAC-SHA-512)	A1420 A2697
		IOS Common Cryptographic Module (IC2M) Rel5a	HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA384, and HMAC-SHA-512)	A1462
FCS_RBG_EXT.1	CTR_DRBG (AES)	CiscoSSL FIPS Object Module (FOM) 7.2a	DRBG CTR_DRBG (AES 256)	A1420 A2697

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
		IOS Common Cryptographic Module (IC2M) Rel5a	DRBG CTR_DRBG (AES 256)	A1462

4.3 Communications

The TOE has the ability to validate the NAS and prevent it from being spoofed. It receives the transmitted Access-Request and identifies where it's sent from. The TOE is able to validate the authenticity of the NAS by verifying the Message Authenticator that is computed in part using a shared secret known to both the NAS and the TOE as defined in RFC 3579. It then returns a valid response to the NAS upon receipt of an Access-Request. The response contains the necessary information to the recipient of that message that identifies the TOE as the valid recipient of the original Access-Request and the Access-Request that elicited the response from the TOE.

4.4 Identification and Authentication

All users wanting to use TOE services are identified and authenticated prior to being allowed access to any of the services other than the display of the warning banner. Once a user attempts to access the management functionality of the TOE, the TOE prompts the user for a user name and password for remote password-based authentication. The identification and authentication credentials are confirmed against a local user database or an optional remote authentication store (part of the IT Environment). Other authentication options include public key authentication. For remote X.509 certificate-based authentication to the administration application, a remote authentication store is required in order to perform the association of the credentials to an ISE role-based access control. For the SSH public key authentication method, the public keys configured by the EXEC CLI command "crypto key import" command will be used for signature verification. The user information is from the local user database. In all cases only after the Administrator presents the correct identification and authentication credentials will access to the TOE functionality be granted. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS/HTTPS connections.

The TOE provides the capability to set password minimum length rules. This is to ensure the use of strong passwords in attempts to protect against brute force attacks. The TOE also accepts passwords composed of a variety of characters to support complex password composition. During authentication, no indication is given of the characters composing the password.

4.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure session, a terminal server or a local console connection. The TOE provides the ability to perform the following actions:

- Administer the TOE locally and remotely
- Configure the access banner
- Configure the cryptographic services
- Update the TOE and verify the updates using digital signature capability prior to installing those updates
- Specify the time limits of session inactivity

All of these management functions are restricted to the Security Administrator of the TOE, which covers all administrator roles (see table for FMT_SMR.2 in Section 6.1 of the ST). The Security Administrators of the TOE are individuals who manage specific type of administrative tasks. The Security Administrators are dependent upon the admin role assigned to them, which limits the network access or tasks they can perform (a role-based access approach).

The primary management interface is the HTTPS Cisco ISE user interface. The Cisco ISE user interface provides an integrated network administration console from which you can manage various identity services. These services include authentication, authorization, posture, guest, profiler, as well as monitoring, troubleshooting, and reporting. All of these services can be managed from a single console window called the Cisco ISE dashboard. The navigation tabs and menus at the top of the window provide point-and-click access to all other administration features. A Command Line Interface (CLI) is also supplied for additional administration functionality like system-level configuration in EXEC mode and other configuration tasks in configuration mode and to generate operational logs for troubleshooting. This interface can be used remotely over SSHv2.

4.6 Protection of the TSF

The TOE can terminate inactive sessions after a Security Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE provides protection of TSF data (authentication data and cryptographic keys). In addition, the TOE internally maintains the date and time. This date and time is used as the time stamp that is applied to TOE generated audit records. This time can be set manually. The TOE is also capable of ensuring software updates are from a reliable source. Finally, the TOE performs testing to verify correct operation.

In order for updates to be installed on the TOE, an administrator must use the digital signature mechanism to confirm the integrity of the product.

4.7 TOE Access

The TOE can terminate inactive sessions after a Security Administrator configurable time-period. The TOE also allows users to terminate their own interactive session. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display a Security Administrator specified banner on the CLI and the web-based management interface prior to allowing any administrative access to the TOE.

4.8 Trusted path/channels

The TOE establishes a trusted path between the ISE and the administrative web-based UI using TLS/HTTPS, and between the ISE and the CLI using SSH. The TOE also establishes a secure connection for sending syslog data to other IT devices using TLS and other external authentication stores using TLS-protected communications.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 4: TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The

Assumption	Assumption Definition
	exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINSTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or

Assumption	Assumption Definition
	intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_ SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ADMINISTRATOR	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

Assumption	Assumption Definition
A.VS_ISOLATON	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.
A.NAS	It is assumed that the TOE is connected to a Network Access Server (NAS) located in the Operational Environment that transmits authentication requests to it.

5.2 Threats

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

Table 5: Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

Threat	Threat Definition
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.

Threat	Threat Definition
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.

Threat	Threat Definition
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.FALSE_ENDPOINTS	A malicious actor may falsely impersonate the TOE or the NAS in order to cause the TOE to operate in an insecure manner or to extract security-relevant data from the TOE or its Operational Environment.
T.INVALID_USERS	A malicious user may supply incorrect credential data or an otherwise invalid authentication request that is approved or ignored by the TSF such that protected resources in the Operational Environment are subject to unauthenticated access.

5.3 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 collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e & Network Device (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0.
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the Hyper V and RedHat instantiations of the product are excluded from the scope of the evaluation as are the features mentioned in Table 6 of Section 7.2.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cisco Identity Services Engine (ISE)v3.1, Common Criteria Operational User Guidance and Preparative Procedures, Version 0.5
- ISE Configuration for EAP-TLS Server, Version 0.2
- Cisco Identity Services Engine CLI Reference Guide, Release 3.1, August 2021
- Cisco Identity Services Engine Administrator Guide, Release 3.1, August 2021
- Cisco Identity Services Engine Installation Guide, Release 3.1, August 2021
- Cisco SNS 3500 Series Appliance Hardware Installation Guide, October 2016
- Cisco SNS 3600 Series Appliance Hardware Installation Guide, February 2019
- Public Key Infrastructure Configuration Guide, Cisco IOS Release 15MT, November 2012

Any additional customer documentation provided with the product, or available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration consists of one ISE instance in a stand-alone deployment when configured in accordance with the documentation specified in Section 6 of this report.

The following figure that shows a typical TOE deployment includes the following components:

- Nodes – An instance of Cisco ISE (SNS appliance or ISE-VM).
- Network devices – The clients that are provided authentication services by ISE
- Endpoints – Devices through which the administrators can log in and manage the TOE.
- Syslog Server - The TOE can be configured to send syslog events to the syslog server.

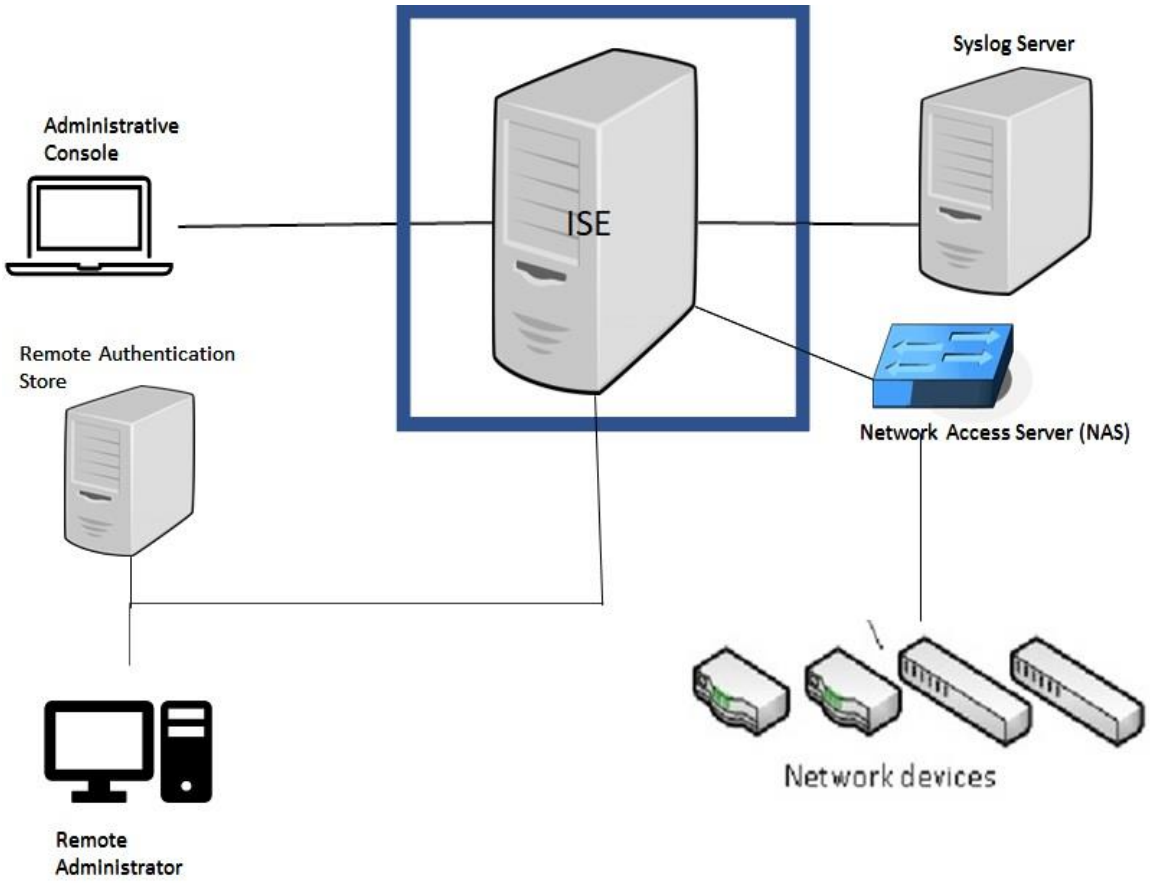

Figure 1: TOE Deployment

- TOE Boundary

The evaluated configuration will include one ISE instance in a network. The TOE deployment will include network devices utilizing the ISE AAA features, remote administrator, local administrative console and a remote authentication store. Both the remote administrator and local administrator console capabilities must be supported.

7.2 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 6: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS mode of operation	This mode of operation includes non-FIPS allowed operations.
Guest Management	Not within the scope of the evaluation
The device profiler feed service	Not within the scope of the evaluation.
NTP	This version of TOE cannot provide secure NTP channel.
Virtual environment Microsoft Hyper-V on Microsoft Windows Server 2012 R2 for ISE-VM	Only ESXi 6.7/7.0 virtual environment will be tested
Virtual environment KVM on RHEL 7.3 for ISE-VM	Only ESXi 6.7/7.0 virtual environment will be tested

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the collaborative Protection Profile for Network Devices Version 2.2e and Network Device (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary ETR for Cisco Identity Services Engine (ISE) V3.1 as summarized in the public AAR. The AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e & Network Device collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0.

The Independent Testing activity including a description of test beds and test tools used is documented in Section 4.1 of the AAR, which is publicly available, and is not duplicated here.

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 documents: Detailed Test Report (DTR) and ETR. The reader of this document can assume that all 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 evaluation determined the Cisco Identity Services Engine (ISE) V3.1 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Identity Services Engine (ISE) V3.1 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e & Network Device collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0.

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.

9.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. 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 ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e & Network Device collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0. related to the examination of the information contained in the 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 Guidance Documents

The evaluation team applied each AGD CEM work unit. 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. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e & Network Device collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0. related to the examination of the information contained in the operational guidance documents.

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 Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. 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 Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e & Network Device collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0. and recorded the results in a Test Report, summarized in the ETR and AAR.

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 collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e & Network Device collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0., and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. A list of the vulnerability databases searched, the search terms used, and the date of the search may be found in Section 7.6 of the AAR.

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 collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e & Network Device collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0, 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 collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e & Network Device collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

All of the validators concerns are adequately captured in Section 5, Assumptions and Clarification of Scope.

In particular, the Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in Cisco Identity Services Engine (ISE) Version 3.1 User Guide, August 2023. No versions of the TOE software, either earlier or later were evaluated.

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.

11 Annexes

Not applicable.

12 Security Target

Cisco Identity Services Engine (ISE) V3.1 Security Target, Version 1.4

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, March 23, 2020 & Network Device collaborative Protection Profile (NDcPP) Extended Package (EP) for Authentication Servers, Version 1.0, August 7, 2015
6. Cisco Identity Services Engine (ISE) V3.1 Assurance Activity Report, Version 0.3
7. Cisco Identity Services Engine (ISE) V3.1 Evaluation Technical Report, Version 0.3
8. Cisco Identity Services Engine (ISE)v3.1, Common Criteria Operational User Guidance and Preparative Procedures, Version 0.5
9. ISE Configuration for EAP-TLS Server, Version 0.2
10. Cisco Identity Services Engine CLI Reference Guide, Release 3.1, August 2021
11. Cisco Identity Services Engine Administrator Guide, Release 3.1, August 2021
12. Cisco Identity Services Engine Installation Guide, Release 3.1, August 2021
13. Cisco SNS 3500 Series Appliance Hardware Installation Guide, October 2016
14. Cisco SNS 3600 Series Appliance Hardware Installation Guide, February 2019
15. Public Key Infrastructure Configuration Guide, Cisco IOS Release 15MT, November 2012
16. Cisco Identity Services Engine (ISE) V3.1 Security Target, Version 1.4