# National Information Assurance Partnership
# Common Criteria Evaluation and Validation Scheme


# Validation Report
# for
# Cisco Identity Services Engine (ISE) V3.3

**Report Number:** CCEVS-VR-VID11517-2025
**Dated:** April 22, 2025
**Version:** 1.0

**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

Jenn Dotson
Randy Heimann
Lisa Mitchell
Clare Parran
Lori Sarem
Chris Thorpe
*The MITRE Corporation*

## Common Criteria Testing Laboratory

Khai Van
*Gossamer Security Solutions, Inc.*
*Columbia, MD*

# Table of Contents

# 1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Identity Services Engine (ISE) V3.3 solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in April 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the *PP-Configuration for Network Devices and Authentication Servers*, Version 1.0, 06 September 2023 (CFG_NDcPP-AUTHSVR_V1.0) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for Authentication Servers*, Version 1.0, 25 January 2023 (AUTHSRV10).

The TOE is the Cisco Identity Services Engine (ISE) V3.3. 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). 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Cisco Identity Services Engine (ISE) V3.3 Security Target*, version 1.0, April 21, 2025 and analysis performed by the Validation team.

# 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 commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 Validated Products 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 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) V3.3 |
| **Protection Profile** | *PP-Configuration for Network Devices and Authentication Servers*, Version 1.0, 06 September 2023 (CFG_NDcPP-AUTHSVR_V1.0) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for Authentication Servers*, Version 1.0, 25 January 2023 (AUTHSRV10) |
| **ST** | *Cisco Identity Services Engine (ISE) V3.3 Security Target*, version 1.0, April 21, 2025 |
| **Evaluation Technical Report** | *Evaluation Technical Report for Cisco Identity Services Engine (ISE) V3.3*, version 1.0, April 21, 2025 |
| **CC Version** | Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5 |
| **Conformance Result** | CC Part 2 extended, CC Part 3 conformant |
| **Sponsor** | Cisco Systems, Inc. |
| **Developer** | Cisco Systems, Inc. |

| Item | Identifier |
|---|---|
| **Common Criteria Testing Lab (CCTL)** | Gossamer Security Solutions, Inc.<br>Columbia, MD |
| **CCEVS Validators** | Jenn Dotson, Randy Heimann, Lisa Mitchell, Clare Parran, Lori Sarem, Chris Thorpe |

# 3 Architectural Information

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

The TOE is an identity and access control platform that enables organizations to enforce compliance and security within the network infrastructure. The TOE includes the following options: Cisco Identity Services Engine Appliances SNS-3715, SNS-3755, SNS-3795 and Cisco Identity Services Engine Virtual Machine (ISE-VM) on ESXi 7.0 running on UCSC-C220-M6S.

## 3.1 TOE Description

The ISE v3.3 TOE is a consolidated policy-based access control system that combines authentication, authorization, accounting (AAA) and guest management in one appliance. ISE v3.3 software runs on the Cisco Application Deployment Engine (ADE) Release 3.3 operating system (ADE-OS). ADE-OS is a Cisco-proprietary Red Hat Enterprise Linux based Operating system [RHEL v8.4 w/Linux kernel 4.18]. The TOE provides IPsec session capabilities to secure the channel between itself and the NAS.

Network access has evolved beyond just simple username 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 SNS supports these applications in three versions. The Cisco SNS 3715 is designed for small deployments. The SNS 3755 and 3795 have several redundant components such as hard disks and power supplies, making them suitable for larger deployments that require highly reliable system configurations.

Apart from the SNS models described above, ISE is also available as a Vitual Machine running on ESXi 7.0 on UCSC-C220-M6S. Cisco ISE supports the following virtual environment platforms, but only the ESXi 7.0 environment is a part of the evaluated configuration:

- ESXi 7.0
- Microsoft Hyper-V on Microsoft Windows Server 2012 R2 and later
- KVM on RHEL 8.4

## 3.2 TOE Evaluated Platforms

| Hardware Models | Cisco Identity Services Engine Appliance 3715 (SNS-3715) | Cisco Identity Services Engine Appliance 3755 (SNS-3755) | Cisco Identity Services Engine Appliance 3795 (SNS-3795) | Cisco Identity Services Engine – VM running on ESXi 7.0/UCSC-C220-M6S (ISE-VM) |
|---|---|---|---|---|
| **Processors** | Intel Xeon Silver 4310 (Ice Lake) | Intel Xeon Silver 4316 (Ice Lake) | Intel Xeon Silver 4316 (Ice Lake) | Intel Xeon Silver 4310 (Ice Lake)[1] |
| **Memory** | 32GB | 96 GB | 256 GB | 96 GB |
| **Hard disk** | 1x600 Gb disk | 4x600Gb disk | 8x600Gb disk | 4x600Gb disk |
| **RAID** | No | Yes (RAID 1+0) | Yes (RAID 1+0) | Yes (RAID 1+0) |
| **Network interface** | 2 x 10GBase-T<br>4 x 10GE SFP<br>(Intel X710) | 2 x 10GBase-T<br>4 x 10GE SFP<br>(Intel X710) | 2 x 10GBase-T<br>4 x 10GE SFP<br>(Intel X710) | Dual 10GBASE-T Ethernet ports (Intel x550) |
| **Hypervisor** | None | None | None | ESXi 7.0 |

## 3.3 TOE Architecture

The evaluated configuration of the TOE includes only one instance of ISE in a stand-alone deployment.

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

- **TOE** – An instance of Cisco ISE (SNS appliance or ISE-VM)/node.
- **Clients** – The network devices 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.

[1] While tested on the Intel Xeon Silver 4310 (Ice Lake), any Intel Xeon processor with the Ice Lake microarchitecture may be used as part of the evaluated configuration with VMware ESXi 7.0

- **Network Access Server** - The Network Access Server is used during the 802.1X authentication exchange as the RADIUS Authenticator to relay the supplicant authentication to the Authentication Server.
- **Remote Authentication Store** - The TOE can be configured to require local authentication and/or remote authentication via a remote authentication store.
- **NTP Server** - The TOE supports communications with an NTP server to synchronize time.
- **OCSP Responder** - OCSP is used to validate the revocation status of the certificates for session establishment.

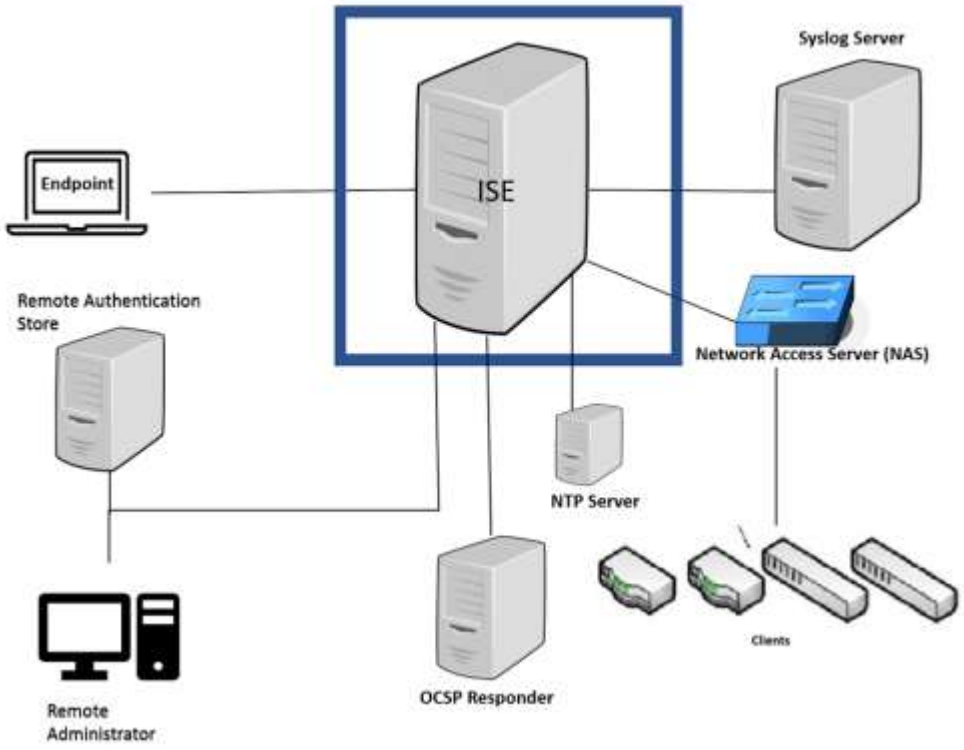


**Figure: TOE Deployment**

- TOE Boundary

## 3.4 Physical Boundaries

The Cisco ISE software includes the Cisco Application Deployment Engine (ADE) Release 3.3 operating system (ADE-OS). The Cisco ISE software run on a dedicated Cisco ISE 3600/3700 Series appliances and on ESXi 7.0 running on Cisco UCS C220-M6S (UCSC-C220-M6S). All models include the same security functionality.

# 4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Communication
4. Identification and authentication
5. Security management
6. Protection of the TSF
7. TOE access
8. Trusted path/channels

## 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 on the ISE administration interface. 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 communication 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, TLS/HTTPS on the server side and TLS on the client side and IPsec session capabilities to secure the channel between the TOE and NAS.

## 4.3 Communication

The TOE can validate the NAS and prevent it from being spoofed. It receives the transmitted Access-Request and identifies from where it is sent. 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 username 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 to perform the association of the credentials to an ISE Role Based Access Control role. 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 revocation status of the certificates can be validated by the TOE using OCSP.

The TOE provides the capability to set password minimum length rules. This is to ensure the use of strong passwords 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 management functions are restricted to the Security Administrator of the TOE, which covers all administrator roles. The Security Administrators of the TOE are individuals who manage specific types 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 to 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 and via NTP. 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. The TOE implements IPsec session capabilities to secure the channel between the TOE and NAS.

# 5 Assumptions & Clarification of Scope

## 5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e)
- *PP-Module for Authentication Servers*, Version 1.0, 25 January 2023 (AUTHSRV10)

That information has not been reproduced here and the NDcPP22e/AUTHSRV10 should be consulted if there is interest in that material.

## 5.2 Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/AUTHSRV10 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 assurance activities specified in the collaborative NDcPP22e and the AUTHSRV10 and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guides, additional customer documentation for the specific Authentication Server models was not included in the scope of the evaluation and, therefore, should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, 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 NDcPP22e/AUTHSRV10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

# 6 Documentation

The following documents were available with the TOE for evaluation:

- Cisco Identity Services Engine (ISE) v3.3 Common Criteria Operational User Guidance and Preparative Procedures, Version 1.0, April 21, 2025
- ISE Configuration for EAP-TLS Server (Supplement to the Common Criteria Operational User Guidance And Preparative Procedures for ISEv3.3), Version 1.0, April 21, 2025
- Configuring Cisco Identity Services Engine Client Certificate Authentication for Administration Application, no version or date provided
- Asset Visibility, no version or date provided
- Cisco Identity Services Engine CLI Reference Guide, Release 3.3, 2025-02-24
- Cisco Identity Services Engine Installation Guide, Release 3.3, 2025-02-03

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.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

# 7 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 *Detailed Test Report for Cisco Identity Services Engine (ISE) V3.3*, Version 1.0, April 21, 2025 (DTR), as summarized in the evaluation *Assurance Activity Report for Cisco Identity Services Engine (ISE) V3.3*, Version 1.0, April 21, 2025 (AAR).

## 7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

## 7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/AUTHSRV10 including the tests associated with optional requirements. The AAR, in Section 3.4.1, lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

# 8 Evaluated Configuration

The evaluated configuration of the TOE includes one ISE instance (see Section 3.2) in a network. As shown in Section 3.3, the evaluated configuration of the TOE includes network devices utilizing the ISE authentication, authorization and accounting (AAA) features, remote administrator, local administrative console and a remote authentication store. Both the remote administrator and local administrator console capabilities must be supported.

# 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 assurance 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) V3.3 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/AUTHSRV10.

## 9.1 Evaluation of the Security Target (ASE)

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) V3.3 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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. 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 and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP22e/AUTHSRV10 related to the examination of the information contained in the TSS.

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.

## 9.3 Evaluation of the Guidance Documents (AGD)

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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

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.

## 9.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

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.

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

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the NDcPP22e/AUTHSRV10 and recorded the results in the proprietary DTR, summarized in the AAR.

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.

## 9.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the DTR prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The Evaluation team searched the:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search),
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/),
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities),
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories),
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search), and
- Offensive Security Exploit Database (https://www.exploit-db.com/)

on 4/14/2025 with the following search terms: "Cisco Identity Services Engine", "ISE 3.3", "ISE SNS 3700", "ISE-VM", "Cisco UCS C220-M6S", "Cisco Application Deployment Engine 3.3", "ADE-OS", "Intel Xeon Silver 4310", "Intel Xeon Silver 4316", "Intel Ice Lake", "CiscoSSL FOM 7.3a", "CiscoSSL FOM", "Cisco FIPS Object Module", "SNS-3715", "SNS-3755", "SNS-3795", "ESXi 7.0".

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.

## 9.7 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 testing 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 followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

# 10 Validator Comments/Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions listed in Section 6. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated. No versions of the TOE and software, either earlier or later, were evaluated. Any additional customer documentation, not listed in Section 6, provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore, should not be relied upon to configure or operate the TOE as evaluated.

The Validation team suggests that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

# 11 Annexes

Not applicable

# 12 Security Target

The Security Target is identified as: *Cisco Identity Services Engine (ISE) V3.3 Security Target,* Version 1.0, April 21, 2025.

# 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, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] *collaborative Protection Profile for Network Devices, Version 2.2e*, 23 March 2020 (NDcPP22e).

[5] *PP-Module for Authentication Servers*, Version 1.0, 25 January 2023 (AUTHSRV10).

[6] *Cisco Identity Services Engine (ISE) V3.3 Security Target*, Version 1.0, April 21, 2025 (ST).

[7] *Assurance Activity Report for Cisco Identity Services Engine (ISE) V3.3*, Version 1.0, April 21, 2025 (AAR).

[8] *Detailed Test Report for Cisco Identity Services Engine (ISE) V3.3*, Version 1.0, April 21, 2025 (DTR).

[9] *Evaluation Technical Report for Cisco Identity Services Engine (ISE) V3.3*, Version 1.0, April 21, 2025 (ETR).