National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Cisco Identity Services Engine (ISE) v2.0

Report Number: CCEVS-VR-10795-2017
Version 1.0
April 13, 2017

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers
Meredith Hennan

The Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Christopher Gugel, CC Technical Director
David Cornwell
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Annapolis Junction, Maryland

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) v2.0 provided by Cisco Systems, Inc. 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 Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Annapolis Junction, Maryland, United States of America, and was completed in April 2017. The information in this report is largely derived from the Evaluation Technical Report (ETR), Assurance Activity Report (AAR), and associated test reports, all written by Booz Allen. 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 Supporting Documents for the collaborative Protection Profile for Network Devices (NDcPP), version 1.0.

The Target of Evaluation (TOE) is the Cisco Identity Services Engine (ISE) version 2.0, running on Cisco Application Deployment Engine (ADE) Release 2.4 operating system (ADE-OS). The physical boundary for the TOE is the following hardware models, each of which can operate as a standalone network appliance:

- ISE 3400 series: SNS-3415 and SNS-3495
- ISE 3500 series: SNS-3515 and SNS-3595

The primary purpose of the device is to act as a network device-based identity, authentication, and access control policy platform that is used to enforce administrative access to other network infrastructure equipment deployed within an organization. However, the evaluated TOE functionality includes only the security functional behavior that is defined in the claimed NDcPP.

The 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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the NDcPP Supporting Documents. This Validation Report applies only to the specific version of the TOE as directed in the *Cisco Identity Services Engine (ISE) Common Criteria Operational User Guidance and Preparative Procedures, Version 0.5, dated January 2017* (AGD). 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 monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR and AAR for the NDcPP Evaluation Activities and CEM work units. 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 *Cisco Identity Services Engine (ISE) Security Target*, *Version 0.8*, dated March 2017 as configured using the *Cisco Identity Services Engine (ISE) Common Criteria Operational User Guidance and Preparative Procedures, Version 0.5, dated January 2017*, and analysis of evaluation evidence 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). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP 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 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 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 ISE v2.0 devices running ADE-OS Release 2.4 *Refer to Table 2 for Models and Specifications
Protection Profile	collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015 (including all applicable NIAP Technical Decisions)
Security Target	Cisco Identity Services Engine (ISE) Security Target, Version 0.8, March 2017
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Cisco Identity Services Engine (ISE) v2.0" Evaluation Technical Report v1.0 dated March 15, 2017
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Annapolis Junction, Maryland
CCEVS Validators	Meredith Hennan, Aerospace Corporation Jerome Myers, Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that the TOE is deployed in a physically secured operational environment and not subjected to any physical attacks.
- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- The TOE is not responsible for protecting network traffic that is transmitted across its interfaces that is not related to any TOE management functionality or generated data.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that regular software and firmware updates will be applied by a TOE Administrator when made available by the product vendor.
- Administrator credentials are assumed to be secured from unauthorized disclosure.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.UNAUTHORIZED_ADMINISTRATOR_ACCESS** – Threat agents may attempt to gain administrator access to the TOE's management functionality through nefarious means such as replay, impersonation, or man-in-the-middle attacks.
- **T.WEAK_CRYPTOGRAPHY** – Threat agents may exploit weak keys or cryptographic algorithms to gain unauthorized access to protected data at rest or in transit.
- **T.UNTRUSTED_COMMUNICATION_CHANNELS** – Threat agents may exploit unencrypted communications channels to access sensitive data or manipulate data in transit.
- **T.WEAK_AUTHENTICATION_ENDPOINTS** – Threat agents may take advantage of secure protocols to access a remote endpoint used by the TOE using shared, static, plaintext, or default credentials.
- **T.UPDATE_COMPROMISE –** Threat agents may exploit an unpatched system or provide a malicious update to the TOE in order to cause a known failure.
- **T.UNDETECTED_ACTIVITY** – A malicious administrator may perform improper activities on the TOE and have the ability to prevent audit records of the activity from being generated or to remove all traces of their activities.
- **T.SECURITY_FUNCTIONALITY_COMPROMISE** – A self-protection mechanism of the TOE may fail or be improperly implemented, allowing a threat agent to access functions or data that were meant to be protected.
- **T.PASSWORD_CRACKING –** A weak administrator password may allow a malicious actor to access administrative functionality through password guessing or brute force exhaustion.
- **T.SECURITY_FUNCTIONALITY_FAILURE –** A component of the TOE responsible for implementing security functionality may fail without administrator awareness.

3.3 Clarification of Scope

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 level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, Version 1.1, 27 February 2015, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP are claimed by the TOE and documented in the ST.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to security functionality 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 NDcPP and applicable Technical Decisions. The network authentication and access control functionality included in the product and described in Section 1.3 of the Security Target 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.
- 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 the process.

The evaluated configuration of the TOE includes the Cisco ISE v2.0 product that is comprised of one or more of the product models listed in Table 2 and includes version 2.0 of the software, running on Cisco Application Deployment Engine (ADE) Release 2.4 operating system (ADE-OS). The TOE includes Base and Advanced licensing but all security functionality is provided in each license – the difference between the two licenses is related to non-security-relevant functionality. In the evaluated configuration, the TOE uses TLS/HTTPS to secure remote web-based administration, SSH to secure remote command-line administration, and TLS to secure transmissions of security-relevant data from the TOE to external entities such as authentication server communications and syslog audit data. The TOE provides a FIPS mode of operation; the non-FIPS mode is excluded from the evaluation. The TOE includes administrative guidance in order to instruct Administrators in the secure installation and operation of the TOE. Adherence to this guidance is sufficient to ensure that the TOE is operated in accordance with its evaluated configuration.

4 Architectural Information

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

4.1 TOE Introduction

Cisco ISE v2.0 is a consolidated policy-based access control system that combines authentication, authorization, accounting (AAA), posture, profiler, and guest management in one appliance.

There are two types of license of ISE - Base and Advanced. For the purposes of this evaluation, all claimed functionality is included in both license types. The Base license includes AAA services, guest lifecycle management, compliance reporting and end-to-end monitoring and troubleshooting. The Advanced license expands on the Base license and enables policy decision based on user and device compliance. The Advanced license features include device profiling, posture services, and security group access enforcement capabilities.

There are seven policy models that can be configured in Cisco ISE to determine how network access is granted to the users requesting access to the network resources. The policies are a set of conditions that must be met in order for access to be granted. The policy models are as follows:

- Authentication Policy – defines the protocols that are used to communicate with the network devices, the identity sources used for authentication, and the failover options.
- Authorization Policy – defines the authorization policies and profiles for specific users and groups of users that have access to the network resources. The policies associate rules with specific user and group identities to create the corresponding profiles. Whenever these rules match the configured attributes, the corresponding authorization profile that grants permission is returned by the policy, network access is authorized accordingly.
- Profiler Policy - provides the unique functionality in discovering, locating, and determining the capabilities of all the attached endpoints (a.k.a identities) on the network. The profiler collects an attribute or a set of attributes of all the endpoints on the network and classifies them according to their profiles.
- Client Provisioning Policy – like the Profiler policy, the TOE looks at various elements when classifying the type of login session through which users access the internal network, including:
    - Client machine operating system and version
    - Client machine browser type and version
    - Group to which the user belongs
    - Condition evaluation results (based on applied dictionary attributes)

  After Cisco ISE classifies a client machine, it uses client provisioning resource policies to ensure that the client machine is set up with an appropriate agent version, up-to-date compliance modules for antivirus and antispyware vendor support, and correct agent customization packages and profiles, if necessary.
- Posture Policy - allows the administrator to check the state (posture) for all the endpoints that are connecting to the network with the corporate security policies for compliance before clients are granted access to protected areas of the network.
- Guest Management – allows guest (visitors, contractors, consultants, or customers) to perform an HTTP or HTTPS login to access a network whether that network is a corporate intranet or the public Internet. The ISE Guest service allows any user with privileges (sponsor) to create temporary guest accounts and to sponsor guests. When a guest user first attaches to the local network, either through a wireless or wired

connection, the user is placed in a segregated network with limited access. The ISE Guest service supports default and customizable guest login portals. The entire process, from user account creation to guest network access, is stored for audit and reporting purposes. It is noted that the guest account is only active for the time specified when the account is created.

- Security Group Access Policy - establishes clouds of trusted network devices to build secure networks. Each device in the ISE SGA cloud is authenticated by its neighbors (peers). Communication between the devices in the SGA cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms.

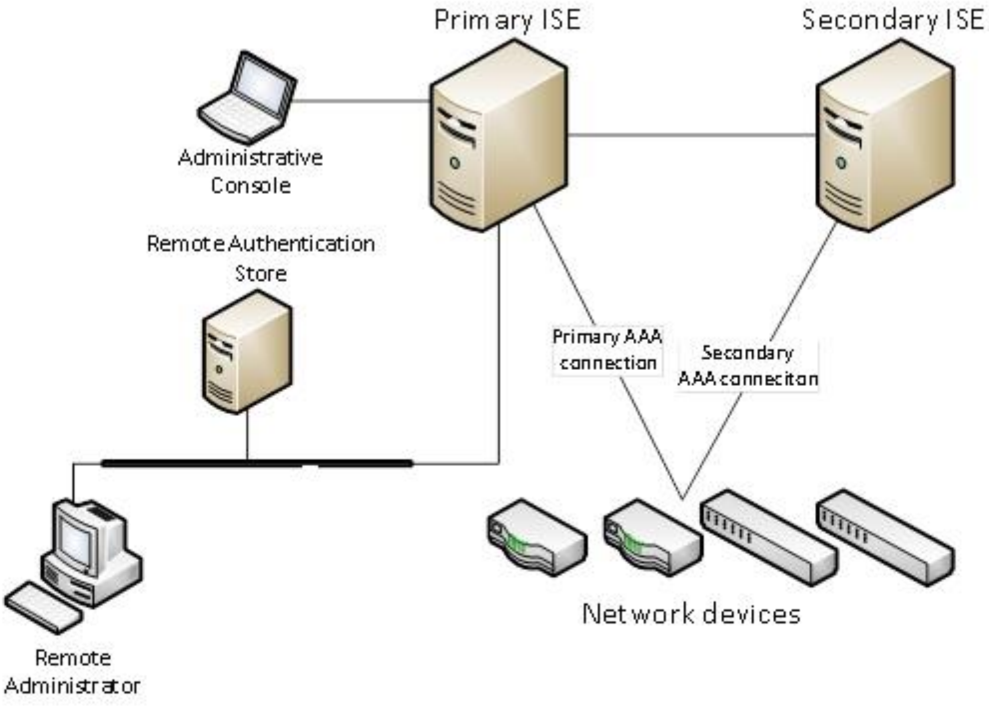
The ISE architecture supports both stand-alone and distributed deployments. In a distributed configuration, one machine assumes the primary role and another "backup" machine assumes the secondary role.

The administrator can deploy ISE nodes with one or more of the Administration, Monitoring, and Policy Service personas, each one performing a different vital part in the overall network policy management topology. Installing ISE with an Administration persona allows the administrator to configure and manage the network from a centralized portal.

The TOE architecture includes the following components:

- Nodes and persona types – A Cisco ISE node can assume the Administration, Policy Service, or Monitoring personas. It can provide various services based on the persona that it assumes.
- Network resources – The clients that are provided authentication services by ISE
- Endpoints – Devices through which the administrators can log in and manage the TOE.

Figure 1: Typical TOE Deployment



The evaluated configuration will include one or more ISE instances in a network. A typical deployment will include 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.

The TOE consists of one or more models as specified below. Each of the models includes ISE version 2.0 software, running on Cisco Application Deployment Engine (ADE) Release 2.4 operating system (ADE-OS).

4.2 Physical Boundaries

The TOE is comprised of both software and hardware. The hardware is comprised of the following:

Table 2 – Hardware Models and Specifications

Hardware Model	Cisco Identity Services Engine Appliance 3415	Cisco Identity Services Engine Appliance 3495	Cisco Identity Services Engine Appliance 3515	Cisco Identity Services Engine Appliance 3595
Processor	Cisco UCS C220M3, Single Intel Xeon E5-2609 4 core processor	Cisco UCS C220M3, Dual Intel Xeon E5-2609 4 core processor (8 cores total)	Cisco UCS C220M4, Single Intel Xeon E5-2620 6 core processor	Cisco UCS 220M4, Dual Intel Xeon E5-2640 8 core processor

Hardware Model	**Cisco Identity Services Engine Appliance 3415**	**Cisco Identity Services Engine Appliance 3495**	**Cisco Identity Services Engine Appliance 3515**	**Cisco Identity Services Engine Appliance 3595**
Memory	16 GB	32 GB	16 GB	64 GB
Hard disk	1x600Gb disk	2x600Gb disk	1x600Gb disk	4x600Gb disk
RAID	Yes (Software RAID level 0 (single drive striped))	Yes (RAID 1)	Yes (Software RAID level 0 (single drive striped))	Yes (RAID 0+1)
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)
Serial port (RJ-45 Connector)	1	1	1	1
USB 2.0 ports	2	2	0	0
USB 3.0 ports	0	0	2	2
1-GB Ethernet Management Port	1	1	1	1
Video ports	1	1	1	1

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 3 – Operational Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Administrative Console (Required)	Yes	Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client to access the CLI or a web browser to access the web GUI. The following web browsers are supported: • Mozilla Firefox version 39 and later • Google Chrome version 43 and later • Microsoft Internet Explorer version 9.x, 10.x, and 11.x – note that some versions of IE will require manually disabling SSL 3.0 and TLS 1.0
Remote Authentication Store (Optional)	No	A third-party LDAP or Active Directory authentication store – note that this is optional because the TOE also supports authentication using locally-defined credentials.
Syslog Target (Required)	Yes	A remote audit server that is capable of receiving syslog data over a TLS-protected channel.

5 Security Policy

This section summarizes the security functionality provided by the Cisco ISE TOE:

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

5.1 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 authorized administrative user, 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 unauthorised 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

5.2 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 key establishment schemes and DH key establishment; digital signature using RSA; cryptographic hashing using SHA1 (and other sizes); random bit generation using DRBG and keyed-hash message authentication using HMAC-SHA (multiple key sizes). The TOE implements the secure protocols - SSH and TLS/HTTPS on the server side and TLS on the client side. The following table contains the CAVP algorithm certificates.

Table 4 –CAVP References

Algorithm	Description	Mode Supported	CAVP Cert. #

Algorithm	Description	Mode Supported	CAVP Cert. #
AES	Used for symmetric encryption/decryption	CBC (128 and 256 bits)	4459
SHS (SHA-1, SHA-256 and SHA-512)	Cryptographic hashing services	Byte Oriented	3672
HMAC (HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512)	Keyed hashing services and software integrity test	Byte Oriented	2959
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	1446
DSA	Signature Verification	FIPS PUB 186-4, “Digital Signature Standard (DSS)”	1192
RSA	Signature Verification and key transport	FIPS PUB 186-4 Key Generation (2048-bit key)	2440
CVL – KAS-FFC	Key Agreement	NIST Special Publication 800-56A	1168

5.3 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 password-based authentication to the administration application, an Active Directory identity source (remote authentication store) is required in order 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 administrative user 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.

5.4 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). 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.

5.5 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.

5.6 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.

5.7 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.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- Cisco Identity Services Engine (ISE) Common Criteria Operational User Guidance and Preparative Procedures, Version 0.5
- Cisco Identity Services Engine CLI Reference Guide, Release 2.0
- Cisco Identity Services Engine Administrator Guide, Release 2.0
- Cisco Identity Services Engine Hardware Installation Guide, Release 2.0

Any additional customer documentation delivered with the product or that is available through download was not included in the scope of the evaluation, and therefore should not be relied upon when configuring or using the products as evaluated.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is one or more Cisco ISE v2.0 standalone network hardware appliances that run software version 2.0, running on Cisco Application Deployment Engine (ADE) Release 2.4 operating system (ADE-OS).

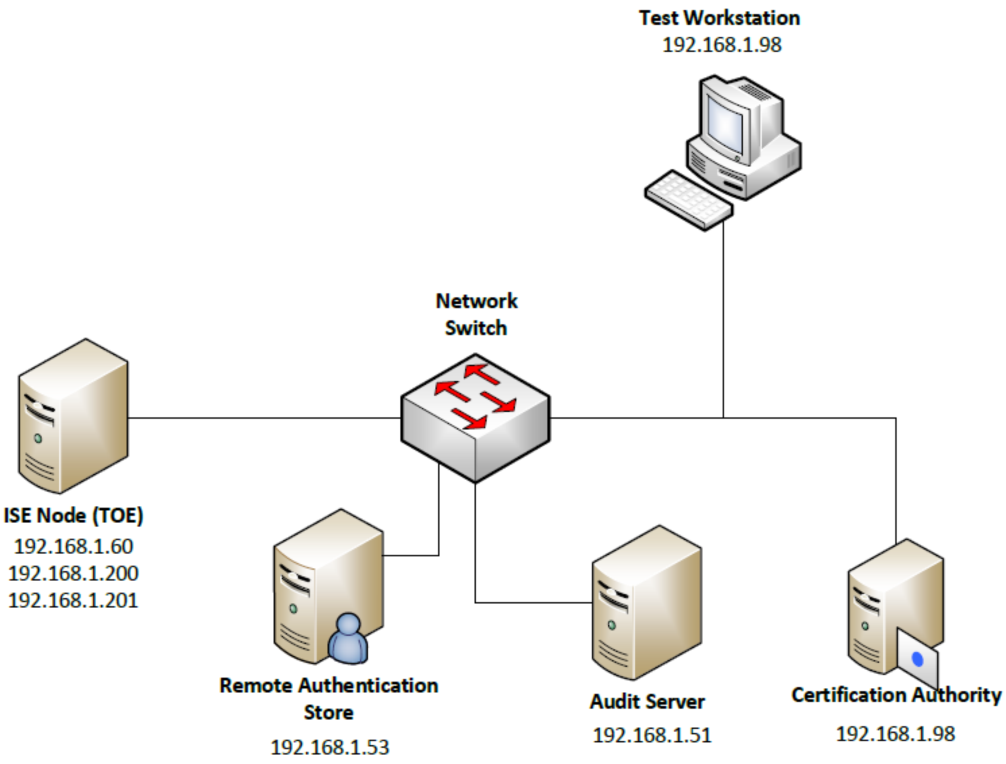
To use the product in the evaluated configuration, the product must be configured as specified in the *Cisco Identity Services Engine (ISE) Common Criteria Operational User Guidance and Preparative Procedures, Version 0.5* document.

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 *Evaluation Technical Report for a Target of Evaluation "Cisco Identity Services Engine (ISE) v2.0" v1.0 dated March 15, 2017*, as summarized in the publically available *Assurance Activity Report for a Target of Evaluation "Cisco Identity Services Engine (ISE) v2.0" Assurance Activities Report v1.0 dated March 15, 2017*.

The following diagram depicts the test environment used by the evaluators.

Figure 2: Evaluator Test Setup



8.1 Test Configuration

The evaluation team configured each tested model of the TOE according the *Cisco Identity Services Engine (ISE) Common Criteria Operational User Guidance and Preparative Procedures, Version 0.5* (AGD) document for testing.

The evaluation team set up a test environment for the independent functional testing that allowed them to perform varying sets of assurance activities against the ISE-3415, ISE-3515, and ISE-3595 models over the SFR relevant interfaces. A sampling strategy was performed such that each test was performed on at least one model and all models had at least one test executed against it. As per the Equivalency Considerations in the NDcPP Supporting Documents, full re-testing of each model is not necessary because the only differences between them are scalability and processing power, neither of which are security-relevant. Since each model uses the same hardware processing family/instruction set and software binary, the different models are considered to be equivalent in terms of security functionality. The overlap in the executed tests showing identical results for each model affirmed this assertion. Based on the architectural arguments for equivalence and the functional testing results, the Booz Allen CCTL has sufficient confidence that the security functionality is identical between each model that the ISE-3495 device is also expected to perform in the same manner as the tested models.

The evaluation team conducted testing in the Booz Allen CCTL facility on an isolated network. Testing was performed against all three management interfaces defined in the ST (local CLI, remote CLI, and remote web GUI). The test sampling strategy ensured that all security relevant functionality that is provided on each interface was tested at least once.

The TOE was configured to communicate with the following environment components:

- Management Workstation for local and remote administration
- Audit Server for recording of syslog data
- Authentication Store (LDAP Server)
- Certificate Authority

The following test tools were installed on a separate workstation (management workstation)

- WireShark: version 2.2.3
- Bitvise SSH Client: version 6.43

*Only the test tools utilized for functional testing have been listed.

8.2 Developer Testing

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

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDcPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov. The following keywords were searched individually and as part of various permutations and combinations: Cisco, ISE, Identity Services Engine, 3415, 3495, 3515, 3595, ADE-OS, and ADE.

Upon the completion of the vulnerability analysis research and initially discovering no known vulnerabilities, the team identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Network Interception – In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network.
- Port Scanning – Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- Web Interface Vulnerability Identification via Burp Suite (OWASP Top 10 vulnerabilities) – Burp Suite is a web application vulnerability assessment tool suite. Burp looks for major vulnerabilities including cross-site scripting, SQL injection, directory traversal, unchecked file uploads, etc. as well as less critical vulnerabilities such as unnecessary information disclosure.
- SSH Downgrade Attack (Force SSHv1) – This attack determines if the TOE will accept SSHv1 connections.

The TOE successfully prevented any attempts of subverting its security.

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 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally the evaluator performed the Evaluation Activities specified in the NDcPP.

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 ISE product 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 NDcPP Supporting Documents in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

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 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 Security Target's TOE Summary Specification. Additionally the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents 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 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents 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 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 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. The evaluation team ran the set of tests specified by the Evaluation Activities in the NDcPP Supporting Documents 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 NDcPP Supporting Documents, 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 evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the NDcPP Supporting Documents were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

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 requirements in the NDcPP Supporting Documents, 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 Evaluation Activities in the NDcPP Supporting Documents, 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 *Cisco Identity Services Engine (ISE) Common Criteria Operational User Guidance and Preparative Procedures, Version 0.5* document.

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 the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Cisco Identity Services Engine (ISE) Security Target, Version 0.8* dated March 2017.

13 List of Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
DH	Diffie-Hellman
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NAC	Network Access Control
OS	Operating System
OSP	Organizational Security Policies
PP	Protection Profile
cPP	Collaborative Protection Profile for Network Devices (NDcPP)
RNG	Random Number Generator
SGA	Security Group Access
SGT	Security Group tags
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VPN	Virtual Private Network
WLC	Wireless LAN Controller

14 Terminology

Term	Definition
Endpoints	An endpoint role is a set of permissions that determine the tasks that the device can perform or services that can be accessed on the Cisco ISE network. Endpoints can be users, personal computers, laptops, IP phones, printers, or any other device supported on the ISE network
Group member	A group member role is a set of permissions that determine the tasks a user (by virtue of being a member of a group) can perform or the services that can be accessed on the ISE network.
Node	A node is an individual instance of ISE.
Persona	The persona of a node determines that service provided by a node. The TOE can be configure as any of the following personas: • Administration – allows the user to perform all of the administrative operations on the TOE. All of the authentication, authorization, auditing, and so on are managed. There can be one or two maximum node instances running the Administration persona and can take any one of the following roles; standalone, primary, or secondary. • Policy Service – provides network access, posture, guest services, client provisioning, and profiling services. This persona evaluates the policies and makes all of the decisions. There can be one or more instance of a node configured as a Policy Service. • Monitoring – functions as the log collector and stores log messages from all of the Administration and Policy Service personas. There can be one or two node instances running the Monitoring persona.
Role	The role identity determines of the TOE is a standalone, primary, or secondary node.
Service	A service is a specific feature that a persona provides, such as network access, posture, security group access, and monitoring
User	A user role is a set of permissions that determine what tasks a user can perform or what services can be accessed on the ISE network. The user identity includes username, password, and group association.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Collaborative Protection Profile for Network Devices, Version 1.0, February 27, 2015.
6. Cisco Identity Services Engine (ISE) Security Target, Version 0.8, March 2017
7. Cisco Identity Services Engine (ISE) Common Criteria Operational User Guidance and Preparative Procedures, Version 0.5, January 2017
8. Evaluation Technical Report for a Target of Evaluation "Cisco Identity Services Engine (ISE) v2.0" Evaluation Technical Report, version 1.0, March 15, 2017
9. Assurance Activities Report for a Target of Evaluation "Cisco Identity Services Engine (ISE) v2.0" Assurance Activities Report (AAR), Version 1.0, March 15, 2017.