Cisco Identity Services Engine (ISE) Security Target

Version 0.8

March 2017

Table of Contents

List of Tables

DOCUMENT INTRODUCTION

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco Identity Services Engine (ISE) v2.0. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Security Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]
- Rationale [Section 7]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 4.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Table 1: ST and TOE Identification

ST Title	Cisco Identity Services Engine (ISE) v2.0 Security Target
ST Version	0.8
Publication Date	March 2017
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Identity Services Engine (ISE) v 2.0
TOE Models	• ISE 3400 series: SNS-3415 and SNS-3495; • ISE 3500 series: SNS-3515 and SNS-3595
TOE Software Version	ISE v2.0, running on Cisco Application Deployment Engine (ADE) Release 2.4 operating system (ADE-OS)
Keywords	AAA, Audit, Authentication, Encryption, NAC, Profiling, Network Device

1.2 Acronyms and Abbreviations

The following acronyms and abbreviations are used in this Security Target:

Table 2: 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

1.3 Terminology

The following terms are used in this Security Target:

Table 3: Acronyms

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

Term	Definition
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.

1.4 TOE Overview

The TOE is an identity and access control platform that enables organizations to enforce compliance and security within the network infrastructure. The TOE includes four hardware options: Cisco Identity Services Engine Appliance 3415, Cisco Identity Services Engine Appliance 3495, Cisco Identity Services Engine Appliance 3515 and Cisco Identity Services Engine Appliance 3595.

1.4.1 TOE Product Type

The Cisco Identity Services Engine (ISE) is a network device identity, authentication, and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline service operations. ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make proactive governance decisions by tying identity to various network elements including

access switches, wireless LAN controllers (WLCs), virtual private network (VPN) gateways, and data center switches.

1.4.2 Supported Non-TOE Hardware/ Software/ Firmware

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

Table 4: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Administrative Console	Yes	This console provides the connection to the ISE appliance for administration and management. The console can connect directly to ISE or over the network via a browser or SSHv2 connection. The TOE supports the following browsers: • Mozilla Firefox version 39 and later • Google Chrome version 43 and later • Microsoft Internet Explorer 9.x, 10.x and 11.x - If using Internet Explorer 10.x, enable TLS 1.1 and TLS 1.2, and disable SSL 3.0 and TLS 1.0 (Internet Options > Advanced.
Remote Authentication Store	No	The TOE supports local authentication or authentication via a remote authentication store, including LDAP and Active Directory.
Syslog Target	Yes	The TOE must offload syslogs to an external entity, which can be another iteration of ISE or a syslog server that supports TLS-protected transfer.

1.5 TOE DESCRIPTION

This section provides an overview of the Cisco Identity Services Engine (ISE) v2.0 Target of Evaluation (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), 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.

1.6 TOE Evaluated Configuration

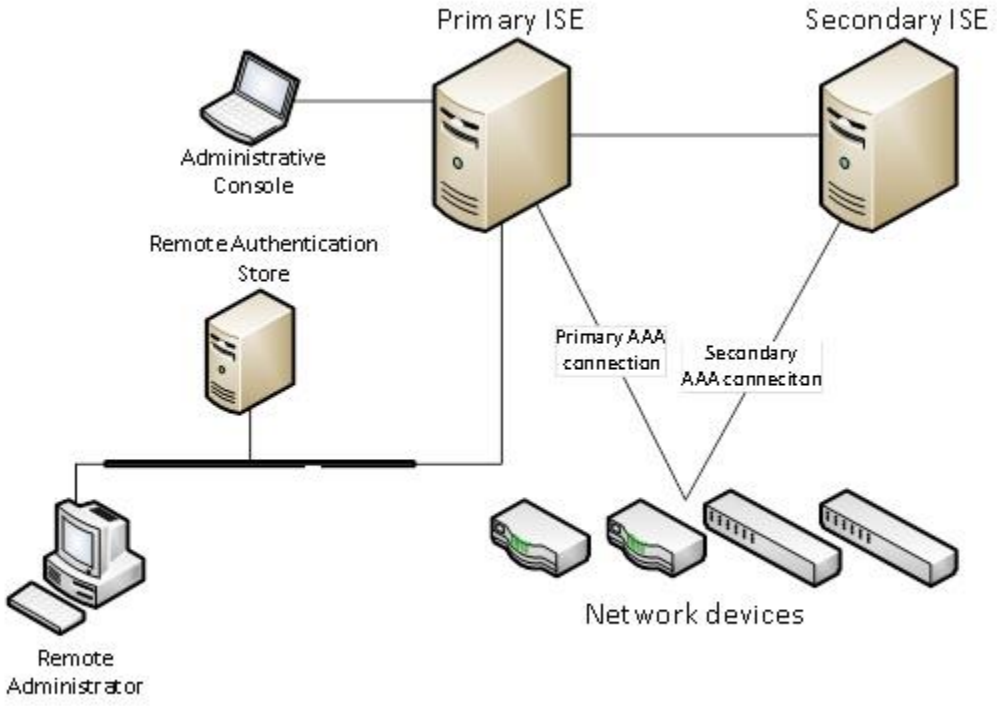
The ISE architecture supports both stand-alone and distributed deployments. In a distributed configuration, one machine assumes the primary role and another “backup” machine assumes the secondary role.

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.

1.7 Physical Scope of the TOE

The Cisco ISE software runs on the Cisco Application Deployment Engine (ADE) Release 2.4 operating system (ADE-OS). The Cisco ADE-OS and Cisco ISE software run on a dedicated Cisco ISE 3400/3500 Series appliance. All models include the same security functionality.

Table 5: TOE Models

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
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

1.8 Logical Scope of the TOE

The NDcPP-compliant 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. Identification and authentication
4. Secure Management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

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

1.8.1 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 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.

1.8.2 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 algorithm certificate references are listed in the table below –

Table 6: CAVP Certificate References

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

1.8.3 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 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.

1.8.4 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.

1.8.5 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.

1.8.6 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.

1.8.7 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.

1.9 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 7: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS mode of operation	This mode of operation includes non-FIPS allowed operations.
All functionalities of Cisco ISE that have not been described in Section 6.1	These functionalities do not map to the NDcPP requirements

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 1.0.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: July 2009. For a listing of Assurance Requirements claimed see Section 5.4. The TOE and ST are CC Part 2 extended and CC Part 3 conformant. The ST is also compliant to the following Technical Decisions –

- TD0125
- TD0130
- TD0143
- TD0156

2.2 Protection Profile Conformance

The TOE and ST are claiming exact conformance to the Protection Profiles listed in Table 8 below:

Table 8: Protection Profiles

Protection Profile	Version	Date
Collaborative Protection Profile for Network Devices (NDcPP)	1.0	February 27, 2015

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the:

- Collaborative Protection Profile for Network Devices (NDcPP), Version 1.0. (Optional SFRs selected include FAU_STG.1, FCS_HTTPS_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.1 and FCS_TLSS_EXT.1

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organizational Security Policies included in the Security Target represent the Assumptions, Threats, and Organizational Security Policies specified in the collaborative Protection Profile for Network Devices, Version 1.0 for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in the NDcPPv1.0, for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the NDcPPv1.0, for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in the NDcPPv1.0.

3 SECURITY PROBLEM DEFINITION

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with "osp" specifying a unique name.

3.1 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 9: 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.
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 computing platform for general purpose applications (unrelated to networking 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 for particular types of network devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	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

Assumption	Assumption Definition
	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.
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.

3.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment.

Table 10: 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.
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.
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.

Threat	Threat Definition
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

Table 11: Organizational Security Policies

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4 SECURITY OBJECTIVES

This section identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

4.1 Security Objectives for the TOE

The collaborative Protection Profile for Network Devices v1.0 does not define any security objectives for the TOE.

4.2 Security Objectives for the Environment

All of the assumptions stated in Section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile non-TOE security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 12: Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	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.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012* and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement made by PP author: Indicated with **bold text** and ~~strikethroughs~~, if necessary;
- Selection: Indicated with underlined text;
- Assignment within a Selection: Indicated with *italicized and underlined text*;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3) and/or by adding a string starting with "/"..
- Where operations were completed in the NDcPP itself, the formatting used in the NDcPP has been retained.
- Formatting used in NDcPP that is inconsistent with the listed conventions has not being retained in the ST.

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs. Formatting conventions outside of operations and iterations matches the formatting specified within the NDcPPv1.0.

5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

Table 13: Security Functional Requirements

Functional Component	
Requirement Class	**Requirement Component**
FAU: Security audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_STG.1: Protected audit trail storage
	FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation
	FCS_CKM.2: Cryptographic Key Establishment
	FCS_CKM.4: Cryptographic Key Destruction

Functional Component	
	FCS_COP.1(1): Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1(2): Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1(3): Cryptographic Operation (Hash Algorithm)
	FCS_COP.1(4): Cryptographic Operation (Keyed-Hash Algorithm)
	FCS_RBG_EXT.1: Random Bit Generation
	FCS_HTTPS_EXT.1: HTTPS Protocol
	FCS_SSHS_EXT.1: SSH Server Protocol
	FCS_TLSC_EXT.1: TLS Client Protocol
	FCS_TLSS_EXT.1: TLS Server Protocol
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management
	FIA_UIA_EXT.1: User Identification and Authentication
	FIA_UAU_EXT.2: Password-based Authentication Mechanism
	FIA_UAU.7: Protected Authentication Feedback
	FIA_X509_EXT.1: X.509 Certificate Validation
	FIA_X509_EXT.2: X.509 Certificate Authentication
	FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security management	FMT_MOF.1(1)/TrustedUpdate: Management of security functions behaviour
	FMT_MOF.1(1)/Audit: Management of security functions behaviour
	FMT_MTD.1: Management of TSF data
	FMT_MTD.1/AdminAct: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1: Protection of Administrator Passwords
	FPT_TST_EXT.1: TSF testing
	FPT_TUD_EXT.1: Trusted update
	FPT_STM.1: Reliable Time Stamps
FTA: TOE Access	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL.4: User-initiated Termination
	FTA_TAB.1: Default TOE Access Banners

Functional Component	
FTP: Trusted path/channels	FTP_ITC.1: Inter-TSF trusted channel
	FTP_TRP.1: Trusted path

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1: Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *All administrator actions comprising:*

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).*
- *Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*
- *Starting and stopping services (if applicable)*
- *[no other actions];*

d) *Specifically defined auditable events listed in Table **14**.*

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *information specified in column three of Table **14**.*

Table 14: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG.1	None.	None.
FAU_STG_EXT.1	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1(1)	None.	None.
FCS_COP.1(2)	None.	None.
FCS_COP.1(3)	None.	None.
FCS_COP.1(4)	None.	None.
FCS_RBG_EXT.1	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
FCS_SSHS_EXT.1	Failure to establish an SSH session Successful SSH rekey	Reason for failure Non-TOE endpoint of connection (IP Address)
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None.	None

Requirement	Auditable Events	Additional Audit Record Contents
FIA_X509_EXT.3	None.	None.
FMT_MOF.1(1)/Audit	Modification of the behaviour of the transmission of audit data to an external IT entity.	None.
FMT_MOF.1(1)/ TrustedUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1	All management activities of TSF data.	None.
FMT_MTD.1/Admin Act	Modification, deletion, generation/import of cryptographic keys.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	No additional information.
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	No additional information.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	No additional information.

Requirement	Auditable Events	Additional Audit Record Contents
FTA_SSL.4	The termination of an interactive session.	No additional information.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

5.2.1.2 FAU_GEN.2: User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 FAU_STG.1: Protected audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

5.2.1.4 FAU_STG_EXT.1: Protected Audit Event Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself.

FAU_STG_EXT.1.3 The TSF shall [overwrite previous audit records according to the following rule: [*when allotted space has reached its threshold*]] when the local storage space for audit data is full.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1: Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- ***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;***
- ***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***

].

5.2.2.2 FCS_CKM.2: Cryptographic Key Establishment

FCS_CKM.2.1 The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- ***RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography";***
- ***Finite field -based key establishment schemes that meets the following: NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"***

].

5.2.2.3 FCS_CKM.4: Cryptographic key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes]]
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that
  - logically addresses the storage location of the key and performs a [single overwrite consisting of [zeroes]]

that meets the following: *No Standard.*

5.2.2.4 FCS_COP.1(1): Cryptographic operation (AES Data Encryption/Decryption)

FCS_COP.1.1(1) The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in* [CBC] mode and

cryptographic key sizes [128 bits, 256 bits] that meet the following: *AES as specified in ISO 18033-3,* [CBC as specified in ISO 10116].

5.2.2.5 FCS_COP.1(2): Cryptographic operation (Signature Generation and Verification)

FCS_COP.1.1(2) The TSF shall perform *cryptographic signature services* (*generation and verification*) in accordance with a specified cryptographic algorithm [

- *RSA Digital Signature Algorithm and cryptographic key sizes **(modulus)** [2048 bits]*

]
that meet the following: [

- *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,*

].

5.2.2.6 FCS_COP.1(3): Cryptographic operation (Hash Algorithm)

FCS_COP.1.1(3) The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA 256, SHA-512] that meet the following: *ISO/IEC 10118-3:2004.*

5.2.2.7 FCS_COP.1(4): Cryptographic operation (Keyed Hash Algorithm)

FCS_COP.1.1(4) The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [*HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512*] and cryptographic key sizes [*160, 256, 512*] bits **and message digest sizes** [***160, 256, 512***] **bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".*

5.2.2.8 FCS_RBG_EXT.1: Cryptographic operation (random bit generation)

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [*CTR_DRBG (AES)*]**.**

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [[*one*] hardware-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength (according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions"), of the keys and hashes that it will generate.

5.2.2.9 FCS_HTTPS_EXT.1: HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

5.2.2.10 FCS_SSHS_EXT.1: SSH

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254, and [6668].

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252:

public key-based, password-based.

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*262144*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: *aes128-cbc*, *aes256-cbc*, [no other algorithms].

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses [SSH_RSA] and **[**no other public key algorithms**]** as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha1] *and* [no other MAC algorithms] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1**]** and [no other methods] are the only allowed key exchange method used for the SSH protocol.

FCS_SSHS_EXT.1.8 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^28 packets have been transmitted using that key.

5.2.2.11 FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] supporting the following ciphersuites:

- *Mandatory Ciphersuites:*
  TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- [*Optional Ciphersuites*:
  - TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
  - TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246

- TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246

].

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The TSF shall only establish a trusted channel if the peer certificate is valid.

FCS_TLSC_EXT.1.4 The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [none] and no other curves.

5.2.2.12 FCS_TLSS_EXT.1 TLS Server Protocol

FCS_TLSS_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] supporting the following ciphersuites:

- *Mandatory Ciphersuites*:

  TLS_RSA_WITH_AES_128_CBC_SHA

- [*Optional Ciphersuites*:
  - TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
  - TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
  - TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246

  ].

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [none].

FCS_TLSS_EXT.1.3 The TSF shall generate key establishment parameters using RSA with key size 2048 bits and [4096 bits] and [Diffie-Hellman parameters of size 2048 bits and [no other size]].

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_PMG_EXT.1: Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a) *Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters:* [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”];

b) *Minimum password length shall be settable by the Security Administrator, and support passwords of 15 characters or greater;*

5.2.3.2 FIA_UIA_EXT.1: User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [no other actions].

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

5.2.3.3 FIA_UAU_EXT.2: Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [*remote password-based mechanism, public-key mechanism*] to perform administrative user authentication.

5.2.3.4 FIA_UAU.7: Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the user while the authentication is in progress at the local console.

5.2.3.5 FIA_X509_EXT.1: X.509 Certificate Validation

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in

RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759].

- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
  - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
  - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
  - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.2.3.6 FIA_X509_EXT.2: X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [TLS], and [no additional uses].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [allow the administrator to choose whether to accept the certificate in these cases].

5.2.3.7 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key and [device-specific information, Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MOF.1(1)/TrustedUpdate: Management of security functions behaviour

FMT_MOF.1.1(1)/TrustedUpdate The TSF shall restrict the ability to enable the functions *to perform manual update to Security Administrators*.

5.2.4.2 FMT_MOF.1(1)/Audit: Management of security functions behaviour

FMT_MOF.1.1(1)/Audit The TSF shall restrict the ability to determine the behaviour of, modify the behaviour of the functions *transmission of audit data to an external IT entity to Security Administrators*.

5.2.4.3 FMT_MTD.1: Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to *manage* the *TSF data* to the *Security Administrators*.

5.2.4.4 FMT_MTD.1/AdminAct: Management of TSF data

FMT_MTD.1.1/AdminAct The TSF shall restrict the ability to *modify, delete, generate/import* the *cryptographic keys* to *Security Administrators*.

5.2.4.5 FMT_SMF.1: Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using* [digital signature] *capability prior to installing those updates;*
- [Ability to configure the cryptographic functionality]

5.2.4.6 FMT_SMR.2: Restrictions on Security roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator*.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely*

are satisfied.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.2.5.2 FPT_APW_EXT.1: Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext passwords.

5.2.5.3 FPT_TST_EXT.1: TSF testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [during initial start-up (on power on)] to demonstrate the correct operation of the TSF: [

- *AES Known Answer Test*
- *RSA Signature Known Answer Test (both signature/verification)*
- *Power up bypass test*
- *DRBG Known Answer Test*
- *HMAC Known Answer Test*
- *SHA-1/256/512 Known Answer Test*
- *Software Integrity Test*

].

5.2.5.4 FPT_TUD_EXT.1: Trusted update

FPT_TUD_EXT.1.1 The TSF shall provide *Security Administrators* the ability to query the current version of the TOE firmware/software as well as the most recently installed version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide *Security Administrators* the ability to manually initiate updates to the TOE firmware/software and [no other update mechanism].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [digital signature mechanism] prior to installing those updates.

5.2.5.5 FPT_STM.1: Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.6 TOE Access (FTA)

5.2.6.1 FTA_SSL_EXT.1: TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [terminate the session] after a Security Administrator-specified time period of inactivity.

5.2.6.2 FTA_SSL.3: TSF-initiated Termination

FTA_SSL.3.1 **Refinement:** The TSF shall terminate **a remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

5.2.6.3 FTA_SSL.4: User-initiated termination

FTA_SSL.4.1 **Refinement:** The TSF shall allow **Administrator**-initiated termination of the **Administrator**'s own interactive session.

5.2.6.4 FTA_TAB.1: Default TOE Access Banners

FTA_TAB.1.1 **Refinement:** Before establishing **an administrative user** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

5.2.7 Trusted Path/Channel (FTP)

5.2.7.1 FTP_ITC.1: Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall be **capable of using [TLS] to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [authentication server]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit **the TSF, or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*all authentication functions, syslogs sent to peer ISE or other devices*].

5.2.7.2 FTP_TRP.1: Trusted path (prevention of disclosure)

FTP_TRP.1.1 The TSF shall **be capable of using [SSH, HTTPS]** to provide a communication path between itself and **authorized remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *disclosure and detection of modification of the channel data*.

FTP_TRP.1.2 The TSF shall permit **remote administrators** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administrative actions**.

.

5.3 TOE SFR Dependencies Rationale

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDcPPv1.0. Guidance from this PP was followed to include selection-based SFRs based on the behavior of the TSF. As such, the NDcPPv1.0 SFR dependency rationale is deemed acceptable since the PP itself has been validated.

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPPv1.0 which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Table 15: Assurance Measures

Assurance Class	Components	Components Description
DEVELOPMENT	ADV_FSP.1	Basic Functional Specification
GUIDANCE DOCUMENTS	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
LIFE CYCLE SUPPORT	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
TESTS	ATE_IND.1	Independent testing - conformance
VULNERABILITY ASSESSMENT	AVA_VAN.1	Vulnerability analysis

5.4.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDcPPv1.0. As such, the NDcPPv1.0 SAR rationale is deemed acceptable since the PP itself has been validated.

5.5 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. The table below lists the details.

Table 16: Assurance Measures

Component	How requirement will be met
ADV_FSP.1	A description of the TOE security functional interfaces (TSFIs) (SFR-enforcing and SFR-supporting TSFIs) that includes the purpose, method of use, and parameters is documented in the Cisco development evidence. The development evidence also contains a tracing of the interfaces to the SFRs described in this ST. The ST and the CC Guidance document contain all of this information.
AGD_OPE.1	The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance.
AGD_PRE.1	Cisco documents the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	Cisco performs configuration management on configuration items of the TOE. Each configuration is uniquely identified and labeled with its unique reference.
ALC_CMS.1	Cisco uniquely identifies configuration items and each release of the TOE has a unique reference. The Configuration Management documentation contains a configuration item list.
ATE_IND.1	Cisco will help meet the independent testing by providing the TOE to the evaluation facility.
AVA_VAN.1	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

This section identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 17: How TOE SFRs are Met

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td>FAU_GEN.1</td><td>The TOE generates and stores audit records locally on the TOE whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, Table 14: Auditable Events. Each of the events is specified in the syslog in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited.
The ability to change logging settings is provided on the Administration > System > Logging > Local Log Settings page.
Following is a sample record: <181>Dec 17 20:17:36 acsview-srv8 CSCOacs_Administrative_Audit 0000003218 1 0 2011-12-17 20:17:36.615 -08:00 0000003936 51001 NOTICE Administrator-Login: Administrator authentication succeeded, ConfigVersionId=3, AdminInterface=GUI, AdminIPAddress=171.69.74.79, AdminSession=058C95A67C4078537C028354A377C11E, AdminName=acsadmin, Each record contains the following fields:
• Category Name—The logging category to which a message belongs (acsview-srv8 in the above record)
• Message Class—The group to which a message belongs (CSCOacs_Administrative_Audit in the above record)
• Message Code—A unique message code identification number associated with a message (0000003218 in the above record)
• Message Text—Name of the message (Administrator-Login in the above record)
• Severity—The severity level associated with a message (NOTICE in the above record)
• Timestamp – The time associated with the message (2011-12-17 20:17:36.615 in the above record)
Note that success or failure is indicated in the individual events, where relevant. The record above indicates that the authentication was successful.
<table>
<tr><th>Auditable Event</th><th>Rationale</th></tr>
<tr><td>Success and failure of encrypted communications (SSH, TLS/HTTPS) and successful SSH rekey</td><td>Attempts of secure encrypted communications/connections (SSH, TLS/HTTPS). The communications include the remote administrator establishing a session and the TOE sending syslog data. The identity of the non-TOE entity is included in the log record.</td></tr>
</table>
</td></tr>
</table>

TOE SFRs	How the SFR is Met	
	All use of the user identification and authentication mechanism.	Events will be generated for attempted identification/ authentication (including whether it was successful or failed), and the username attempting to authenticate will be included in the log record, along with the origin or source of the attempt.
	Unsuccessful attempt to validate a certificate	The reason for failure of certificate validation attempts is logged.
	Changes to the time.	Changes to the time are logged, including old and new values for time, as well as origin of attempt
	Initiation of an update to the TOE.	TOE updates and the result of the update attempts are logged as configuration changes.
	Termination of a remote session.	Termination of a remote session (due to inactivity) is logged (as a terminated cryptographic path).
	Termination of an interactive session.	Termination of an Interactive session (due to logging off) is logged (as the session ending).
	Initiation, termination and failures in trusted channels.	Requests for encrypted session negotiation are logged (including whether successful or failed). Similarly, when an established cryptographic channel or path is terminated or fails a log record is generated. Also the initiator and target of any failed attempts to establish a trusted channels are identified.
	Initiation, termination and failures in trusted paths.	Requests for encrypted session negotiation are logged (including whether successful or failed). Similarly, when an established cryptographic channel or path is terminated or fails a log record is generated. The records include the claimed user identity.
	All management activities of TSF data (e.g. Modification of the behaviour of the transmission of audit data to an external IT entity; Any attempt to initiate a manual update; Modification, deletion,	The use of the security management functions are logged, along with the origin or source of the attempt.

TOE SFRs	How the SFR is Met
	generation/import of cryptographic keys The TOE also sends audit logs to other entities (including other ISE nodes) using TLS protected syslog. ISE is configured by default to listen for UDP, TCP, and TLS-protected TCP. To configure this transfer to use TLS, the administrator must configure the secondary ISE box to send syslogs to the primary ISE via the "System" -> "Logging" tab, and set it to use "Secure Syslog" for the "Target Type". One can obtain reports on the log collection status for all Cisco ISE nodes. Log collection errors are noted by alarms via the dashboard.
FAU_GEN.2	The TOE ensures that each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. Refer to the Guidance documentation for configuration syntax and information.
FAU_STG.1 FAU_STG_EXT.1 FMT_MOF.1(1)/Audit	The TOE stores its own syslog events locally on the platform, and can offload events to other entities (including other ISE nodes) over TLS protected syslog on demand The Security Administrators can configure securing the syslog data using TCP. TCP syslog buffers events in a local file that is limited to a total of 100MB. The limit is specified as a file size, not a specific number of events. Overwriting is handled by wrapping to the beginning of the file (overwriting the oldest events). By default upon adding the remote logging target through the GUI, the remote logging target is enabled. The audit events are not sent to the remote logging target until the administrator has configured which type of logging audit records need to be sent. On the TOE, the local log files rotate after a certain size threshold is reached. The number of days of local log files is configurable, with the default of keeping records only up to last 7 days. From the Administration > System > Logging > Local Log Settings page an administrator is able to configure the storage period for logs in days and delete the existing log file. Only the Security Administrator may delete all of the rolled over log files by the "Delete Local Logs Now" selection in the administration application. The ISE RBAC (Role-Based Access Control) policy does not allow for any user that is not a Security Administrator to delete log files. No user can modify log files because there is no mechanism that allows this.

TOE SFRs	How the SFR is Met
	After the configured storage period of time has passed for logs the events exceeding the age are deleted. The administrators that are able to view the logs (at Operations > Reports > Catalog) are Super Admin, Monitoring Admin, or Helpdesk Admin. The administrator can also set the reports on peer ISE nodes, which is where the TOE stores remote syslog records that are received, to be maintained for a set number of days or delete them immediately if space becomes an issue using commands at the CLI.
FCS_CKM.1 FCS_CKM.2	The TOE implements a FIPS-approved Deterministic Random Bit Generator for RSA key establishment schemes (conformant to NIST SP 800-56B). The RSA keys used in cryptographic operations are generated according to FIPS PUB 186-4 (CAVP Cert # 2440). The RSA schemes using key sizes of 2048 bits meet the FIPS PUB 186-4. Asymmetric cryptographic keys are generated also in accordance with the FFC schemes using cryptographic key sizes of 2048 bits or greater that meet the FIPS 186-4, Digital Signature Standard. The TOE does not implement elliptic-curve-based key establishment schemes. (CAVP Cert # 1192) The cryptographic key establishment is implemented in the TOE according to the RSA-based schemes that meet the NIST SP 800-56B for TLS, SSH and digital signatures and Finite-field based schemes (CAVP Cert # 1168) that meet NIST SP 800-56A for TLS and SSH.
FCS_CKM.4	The TOE meets all requirements for destruction of keys and Critical Security Parameters (CSPs) in that none of the symmetric keys, pre-shared keys, or private keys are stored in plaintext form. The secret keys used for symmetric encryption, private keys, and CSPs used to generate keys, are zeroized immediately after use, or on system shutdown. See Table 18, below for more information. This is followed by a read-verify, which if fails, leads to zerioization process repeating. The AES key that is used to encrypt these other keys stored in the DRAM. The plaintext keys stored on the hard disk drive can be destroyed completely by overwriting the hard disk drive with zeroes and this is accomplished by the *Perform System Erase* utility.
FCS_COP.1(1)	The TOE provides symmetric encryption and decryption capabilities using AES (as specified in ISO 18033-3), in CBC mode (as specified in ISO 10116) with key sizes of 128 bits and 256 bits (CAVP Cert # 4459). These key sizes are used for both TLS and SSH. The AES CAVP certificate number is listed in Table 6: CAVP Certificate References
FCS_COP.1(2)	The TOE will provide cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 bits that meets the FIPS 186-4 Digital Signature Standard. The ISE product can be configured to generate key sizes of 1024 bit, but administrative guidance for the evaluated configuration instructs administrators to only use keys with size 2048.
FCS_COP.1(3)	The TOE provides cryptographic hashing services using SHA-1, SHA-256 and SHA-512. SHA-256 and SHA-512 are used for generating certificate signing requests or generating self-signed certificates on the TOE. SHA-1 and SHA-256 are used for TLS and SSH. (CAVP Cert # 3672)

TOE SFRs	How the SFR is Met
FCS_COP.1(4)	The TOE provides keyed-hashing message authentication services using HMAC-SHA-1(key size – 160 bits, block size 512 bits), HMAC-SHA-256 (key size – 256 bits, block size 512 bits) and SHA-512 (key size -512 bits, block size 1024 bits) and meets the ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2" standard. Note that HMAC-SHA-1 is used for SSH connections, while HMAC-SHA-1 and HMAC-SHA-256 are used for TLS. The MAC lengths for HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512 are 160, 256 and 512 bits respectively. (CAVP Cert # 2959)
FCS_RBG_EXT.1	The TOE implements a random bit generator (RBG) based on the AES-256 block cipher, in accordance with ISO/IEC 18031:2011. The appliance form factor TOE uses the Emulex Pilot III BMC chips. The RBG for the ISE appliance form-factor is seeded with a hardware-based noise source that uses a ring oscillator jitter based architecture that provides 256 bits of minimum entropy. (CAVP Cert # 1446)
FCS_HTTPS_EXT.1	The TOE provides HTTPS, as specified in RFC 2818, to provide a secure interactive interface for remote administrative functions, and to support secure exchange of user authentication parameters during login. HTTPS uses TLS to securely establish the encrypted remote session. The sessions are not established with invalid certificates. Note that port 80 is exposed on the product, but only as a redirect to port 443. HTTP connections are not allowed.
FCS_SSHS_EXT.1	The TOE implements SSHv2. There is no SSHv1 or telnet implementation on the TOE. SSH connections will be dropped if the TOE receives a packet larger than 262,144 bytes. Large packets are detected by the SSH implementation, and dropped internal to the SSH process. The TOE implementation of SSHv2 supports the following public key algorithm for authentication - RSA Signature Verification. The TOE supports RSA public-keys and password-based authentication for administrators accessing the TOE through SSHv2. The TOE implementation of SSHv2 supports the following encryption algorithms - AES-128-CBC, AES-256-CBC to ensure confidentiality of the session. The TOE's implementation of SSHv2 supports hashing algorithm HMAC-SHA1. SSH connection are rekeyed before 2^28 packets have been transmitted using that key. Note that the TOE complies with RFCs 4251, 4252, 4253, 4254 and 6668. DH Group 14 is the only allowed key exchange method used for SSH protocol.
FCS_TLSS_EXT.1 FCS_TLSC_EXT.1	The TOE implements TLS 1.1, conformant to RFC 4346 and TLS 1.2, conformant to RFC 5246 and supports the mandatory ciphersuite- • TLS_RSA_WITH_AES_128_CBC_SHA The optional ciphersuites supported are – • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_ SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 (client only)

TOE SFRs	How the SFR is Met
	• TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 (client only) All connections from clients requesting SSL2.0, SSL3.0 and TLS1.0 are denied. The TOE only supports standard extensions, methods, and characteristics. TLS is used for HTTPS/TLS for management purposes and to establish encrypted sessions with other instances of the TOE and IT entities to send/receive audit data. The trusted channel is established only when the peer certificate is valid. LDAPS has support for additional extensions to support communication with external authentication stores. The TOE verifies that the presented identifier matches the reference identifier according to RFC 6125. When the TOE acts as a TLS client to LDAPS servers, it obtains the RFC 6125 reference identifiers from the administrator configured value in the LDAP Identity Source Hostname/IP field. (Administration application. Menu: Administration > Identity Management > External Identity Sources. Left-Navigation: LDAP. "Connection" tab. Hostname/IP field) When the TOE acts as a TLS client to TLS Secure Syslog servers, it obtains the reference identifiers from the administrator configured value in the Remote Logging Targets **IP/Host Address** field. (Administration application. Menu: Administration > System > Logging. Left-Navigation: Remote Logging Targets. IP/Host Address field). The TOE supports the following presented identifier types: a) subjectAltName entry of type dNSName (DNS-ID in RFC 6125) b) CN-ID as defined in RFC 6125, c) subjectAltName entry of type iPAddress; and d) Wildcards in DNS domain names. Certificate pinning is unsupported by the TOE. The keys establishment parameters are generated using RSA with key sizes 2048 bits and 4096 bits and DH with 2048 bits. Keyed-hashing message authentication services HMAC-SHA-1 and HMAC-SHA-256 are supported for TLS.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). Minimum password length is settable by the Security Administrator, with a default of six characters and can be configured for minimum password lengths of 15 characters or greater. It is configured via the Administration menu in the web-based UI, on the Admin Actions tab, under Password Policy.
FIA_UIA_EXT.1	The TOE requires all users to be successfully identified and authenticated before allowing any services and/or TSF mediated actions to be performed (other than the display of the warning banner) per the authentication policy. A pre-authentication banner is also displayed at both the CLI and GUI. Access to the web-based interface (via HTTPS), the CLI (SSH), and the console, all require at a minimum username and password be provided and successfully verified prior to access being granted. A successful login requires a correct username and password pair be confirmed, as existing in the local user database or a remote authentication store. The SSH interface supports authentication using SSH keys which are provided during the SSH connection request.

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td></td></tr>
<tr><td>FIA_UAU_EXT.2</td><td>The TOE can be configured to require local authentication and/or remote authentication via a remote authentication store as defined in the authentication policy.

The process for authentication is the same for administrative access whether administration is occurring via the HTTPS web-based interface or via SSHv2 at the CLI. At initial login, the administrator is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password or public-key associated with the user account. The TOE then either grants administrative access (if the combination of username and password or public-key is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.

The table below summarizes the authentication mechanisms that are supported at each interface.
<table>
<tr><th>Interface</th><th>Authentication Mechanism</th></tr>
<tr><td>Web-Based (GUI)</td><td>• local password-based (administrator credentials stored locally)
• remote password-based (administrator credentials stored remotely)</td></tr>
<tr><td>Remote SSH (CLI)</td><td>• SSH public key
• local password-based
• remote password-based</td></tr>
<tr><td>Local Console (CLI)</td><td>• local password-based
• remote password-based</td></tr>
</table>
</td></tr>
<tr><td>FIA_UAU.7</td><td>When a user enters their password at the ISE web-based interface only ‘*’ characters are displayed and at the CLI nothing is displayed so that the user password is obscured. Also, the error displayed for the user does not give clues about which part of the credentials entered for authentication failed.</td></tr>
<tr><td>FIA_X509_EXT.1

FIA_X509_EXT.2

FIA_X509_EXT.3</td><td>The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections to the audit server and the authentication server. When a certificate is imported/added in to the TOE, the purpose for which the certificate is to be used needs to be specified -
• Admin: For internode communication and authenticating the Admin portal
• EAP: For TLS-based EAP authentication
• Portal: For communicating with all Cisco ISE end-user portals
Different certificates from each node for communicating with the Admin portal (Admin) and for TLS-based EAP authentication (EAP) can be associated. However, only one certificate from each node for each of these purposes can be associated.</td></tr>
</table>

TOE SFRs	How the SFR is Met
	The certificate path is validated by ensuring that all the CA certificates has the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate. The extendedKeyUsage field is validated according to the rules listed in Section 5.2.3.5. The certificates themselves provide protection in that they are digitally signed. If a certificate is modified in any way, it would be invalidated. The digital signature verifications process would show that the certificate had been tampered with when the hash value would be invalid. The physical security of the TOE (A.PHYSICAL_PROTECTION) protects the router and the certificates from being tampered with or deleted. In addition, the TOE identification and authentication security functions protect an unauthorized user from gaining access to the TOE. OCSP and CRL revocation checking is performed when authenticating a certificate provided by the remote server during TLS establishment. Both OCSP and CRL may be used to validate the revocation status of the certificates when ISE acts as a Secure LDAP (LDAPS) client to LDAPS servers. For all other cases, it's only CRL that is supported to validate the certificate revocation status. Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. If they are not, the certificate is not accepted. When the connection to determine the validity of the certificate cannot be established, the TOE allows the administrator to either accept/not accept the certificate based on the following conditions - a. accept the certificate when: 1. the CRL revocation HTTP download fails with the ISE configuration setting 'Bypass CRL Verification if CRL is not Received' is checked. (e.g., the CRL Distribution HTTP URL server host is unreachable. CRL download receives an HTTP 500 error) 2. OCSP revocation checks on LDAPS client connections fail and the ISE configuration contains the two checkboxes unchecked: Reject the request if OCSP returns UNKNOWN status; and Reject the request if OCSP Responder is unreachable b. not accept the certificate when: 1. the CRL revocation HTTP download fails with the ISE configuration setting 'Bypass CRL Verification if CRL is not Received' is unchecked. 2. OCSP revocation checks on LDAPS client connections fail and the ISE configuration contains the two checkboxes checked: Reject the request if OCSP returns UNKNOWN status; and Reject the request if OCSP Responder is unreachable. If the connection to determine the certificate validity cannot be established, the administrator is able to choose whether or not to accept the certificate. A Certificate Request Message can be generated as specified by RFC 2986 and provide the following information in the request – public key, device-specific information (Node, city and state), Common Name, Organization,

TOE SFRs	How the SFR is Met
	Organizational Unit and Country. The TOE can validate the chain of certificates from the Root CA when the CA Certificate Response is received
FMT_MOF.1(1)/TrustedUpdate FMT_MTD.1	The TOE restricts the ability to enable the functions to perform manual update to the Security Administrator. The TOE restricts access to the management functions to the Security Administrator. The TOE supports two levels of administrators, the CLI-admin (local console or SSHv2 accessible) and the web-based admin user. The same functionality is available on the TOE via the web-based interface and CLI, with the exception that only the CLI-admin can start and stop the ISE application and reload (update) or shutdown the ISE appliance via the CLI. None of the administrative functions of the product are available prior to administrator log-in.
FMT_SMF.1 FMT_MTD.1/AdminAct	The TOE provides all the capabilities necessary to securely manage the TOE, the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI or HTTPS web-based interface. The specific management capabilities available from the TOE are identified in the text of the SFR - FMT_SMF.1. The Security administrator have the ability to generate, delete and import/export cryptographic keys.
FMT_SMR.2	Cisco ISE provides role-based access control (RBAC) policies that ensure security by restricting administrative privileges. RBAC policies are associated with default admin groups to define roles and permissions. A standard set of permissions (for menu as well as data access) is paired with each of the predefined admin groups, and is thereby aligned with the associated role and job function. RBAC restricts system access to authorized users through the use of roles that are then associated with admin groups. Each admin group has the ability to perform certain tasks with permissions that are defined by an RBAC policy. Policies restrict or allow a person to perform tasks that are based on the admin group (or groups) to which that person is assigned. A user can be assigned to multiple roles, which provides them with privileges for each role to which they are assigned. A specialized role has the ability to customize permissions and admin groups and to create custom policies. The default Cisco ISE RBAC policies cannot be modified, however. An individual who manages or performs a specific type of administrative task using the Cisco ISE user interface is considered an admin (or administrator). 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). Using the Cisco ISE user interfaces (CLI and web-based), administrator roles can perform the following tasks: • Change admin or user passwords • Manage deployments, helpdesk operations, monitoring and troubleshooting nodes, and network devices • Manage Cisco ISE services policies and admin access, Cisco ISE administrator accounts and roles, Cisco ISE administrative functions, and Cisco ISE system configuration and operations

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
The TOE supports two categories of administrators, the CLI-admin and the web-based admin user.

The CLI-admin user and the web-based admin user can perform the following ISE system-related tasks:

Backup and restore the Cisco ISE application data
Display any system, application, or diagnostic logs on the Cisco ISE appliance
Apply Cisco ISE software patches, maintenance releases, and upgrades

Following are the default roles for the web-based admin and their capabilities.

Web-based Admin Group Role Descriptions
<table>
<tr><td>Helpdesk Admin</td><td>This role provides access for querying all monitoring and troubleshooting operations and within the Cisco ISE administrative console, and can perform the following tasks:
• Run all reports
• View the Cisco ISE dashboard and livelogs
• View alarms
This role cannot create, update, or delete reports, troubleshooting flows, live authentications, or alarms.</td></tr>
<tr><td>Identity Admin</td><td>This role provides access for managing all of the internal user identities that use the Cisco ISE administrative console across the Cisco ISE network. This role has read and write permissions on identities, endpoints, and identity groups (user identity groups and endpoint identity groups).</td></tr>
<tr><td>Network Device Admin</td><td>This role provides access for Cisco ISE administrators that manage only the Cisco ISE network device repository and perform tasks such as adding, updating, or deleting devices. This role has the following permissions:
• Read and write permissions on network devices
• Read and write permissions on NDGs and all network resources object types</td></tr>
<tr><td>Policy Admin</td><td>This role provides access for Cisco ISE policy administrators who are responsible for creating and managing the policies for all Cisco ISE services across the network that are related to authentication, authorization, posture, profiler, and client provisioning. This role has the following permissions:
• Read and write permissions on identities, endpoints, and identity groups (user identity groups and endpoint identity groups)</td></tr>
<tr><td>RBAC Admin</td><td>This role provides full access (read and write permissions) to perform all activities under the</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>Operations tab and partial access to some menu items under the Administration tab. This role has the following permissions:
• View the authentication details
• Enable or disable endpoint protection service
• Read permissions on administrator account settings and admin group settings</td></tr>
<tr><td>Super Admin</td><td>This role provides access to every Cisco ISE administrative function. This role is assigned to the default administrator account, and has create, read, update, delete, and eXecute (CRUDX) permissions on all Cisco ISE resources.</td></tr>
<tr><td>System Admin</td><td>This role provides access for Cisco ISE administrators who are responsible for Cisco ISE configuration and operations.
This role provides full access (read and write permissions) to perform all activities under the Operations tab and partial access to some menu items under the Administration tab. This role has the following permissions:
• Read permissions on administrator account settings and administrator group settings
• Read permissions on admin access and data access permissions along with the RBAC policy page.
• Read and write permissions for all options under the Administration > System menu.
• View the authentication details
• Enable or disable endpoint protection service
• generate and view reports</td></tr>
</table>

Only the CLI-admin user can perform the following Cisco ISE system-related tasks:
• Start and stop the ISE application software
• Reload or shutdown the ISE appliance
Because only the CLI-admin user can perform these services, the CLI-admin user credentials must be protected. It is noted that only a user assigned these privileges can access the ISE CLI.

The ability to administer the TOE locally is provided through a console connection to the appliance or hardware hosting the software-only instance. The ability to administer the TOE remotely is provided via SSH protected access to the ISE CLI or TLS protected access to the web-based interface.

The ‘Security Administrator’ specified in the SFRs is synonymous/equivalent to the entire set of TOE administrative levels/administrators.</td></tr>
<tr><td>FPT_SKP_EXT.1</td><td>The TOE by default secures all locally defined user passwords using SHA256 hashing for CLI passwords, and AES encryption for GUI credentials. In this</td></tr>
</table>

TOE SFRs	How the SFR is Met
FPT_APW_EXT.1	manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. The TOE stores all private keys in a secure directory that is not accessible to administrators. There is no way an administrator can access/view the private keys in the secure directory where they are stored. All pre-shared and symmetric keys are stored in encrypted (AES) form to prevent access. TOE is designed specifically to not disclose any keys stored in the TOE. All pre-shared and symmetric keys are stored in encrypted form using AES encryption to additionally obscure access. The AES key used for this encryption is stored on the filesystem and in DRAM.
FPT_STM.1	The TOE provides a source of date and time information, used in audit timestamps. This function can be configured from the Administration > System > Settings > System Time page by a Super Admin or System Admin role only. The clock function is reliant on the system clock provided by the underlying hardware. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time information is also used to set system time, determining AAA timeout, administrative session timeout and checking for expiry of certificates.
FPT_TST_EXT.1	ISE runs a suite of self-tests during the TOE initial start-up to verify its correct operation. These tests check the integrity of the code, and the correct operation of each cryptographic algorithm and method used (i.e. AES-CBC, SHA-1, etc.) If any of the tests fail, the administrative web-based UI will not be accessible, and the security administrator will for a limited time window be able to login to the CLI on the KVM (keyboard, video, mouse) console to run the CLI command – "*show application status ise*" to determine that services have been disabled because "FIPS INTEGRITY CHECK HAS FAILED". Eventually the administrator will be unable to login to the CLI even on the KVM as all services are shutdown including the ability to login to the CLI. After authenticating, a fatal error is displayed and the user is only allowed to press <Enter> to logout and no other actions can be performed. The error message is: "ERROR: ISE SERVICES HAVE BEEN DISABLED BECAUSE FIPS INTEGRITY CHECK HAS FAILED! EITHER REIMAGE FROM ISE INSTALLATION MEDIA, OR CONTACT CISCO TECHNICAL SUPPORT CENTER FOR INSTRUCTIONS ON DIAGNOSING THE FAILURE. Press <Enter> to logout". If the tests pass successfully the FIPS badge is displayed on the web-based screen and the web-based UI will be accessible for login by the security administrator. The self-tests include: **AES Known Answer Test** - With a known input and output, the AES algorithm implementation is tested by comparing the result with the expected result. This is done separately for both encryption and decryption. **RSA Known Answer Test** – With a known input and output, the RSA signature service algorithm is tested by comparing the result with the expected result. This is done separately for both signing and verification. **DRBG Known Answer Test -** (CTR_DRBG KAT) – With known input and output, the DRBG computation is tested by comparing an expected pre-computed and stored result against the result computed at runtime.

TOE SFRs	How the SFR is Met
	HMAC Known Answer Test - This includes the HMAC-SHA1 KAT, HMAC-SHA256KAT and HMAC-SHA512 KAT. With a known input and output, the keyed-hash message authentication using each of the HMAC-SHA1, HMAC-SHA256 and HMACSHA512 algorithms is tested by comparing the result with the expected result. **SHA-1/256/512 Known Answer Test** - With a known input and output, the cryptographic hashing service implementation using each of the SHA1, SHA256 and SHA512 algorithms is tested by comparing the result with the expected result. **Software Integrity Test (HMAC-SHA1) -** The HMAC-SHA1 value of the module is computed and compared to the correct already-computed HMAC-SHA1 value for verification. These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected.
FPT_TUD_EXT.1	The TOE has specific versions that can be queried by an administrator from the CLI using the "show version" command, or from the administration GUI, lower left "Help" > About Identity Services Engine. When updates are made available by Cisco, an administrator (specifically the Super Admin or System Admin) can manually obtain the updates from the Cisco website and install them. Digital Signature mechanism is used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. The updates can be downloaded from the software.Cisco.com. The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded. The digital certificates used by the update verification mechanism are contained on the TOE. Detailed instructions for how to do this verification are provided in the administrator guidance for this evaluation. Logs for update actions are located in Operations > Reports > Catalog > Server Instance Report.
FTA_SSL_EXT.1 FTA_SSL.3 FTA_SSL.4	An administrator can configure maximum inactivity times for both local and remote administrative sessions. When a session is inactive (i.e., no session input) for the configured period of time the TOE will terminate the session, requiring the administrator to log in again to establish a new session when needed. At the CLI, once the administrator establishes a new session, they have the option of seeing data from their previous sessions. This is selected after successful authentication and only gives access to that user's previous sessions. The ability to configure these settings is limited to the Super Admin or System Admin. It is configured via the Administration > System > Admin Access > Settings > Session Timeout page. Each administrator logged onto the TOE can manually terminate her session using the "LogOut" link in the web-based or the "exit" or "forceout <username>" commands at the CLI.

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td>FTA_TAB.1</td><td>The TOE displays a privileged Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE. The TOE also displays a banner at the web-based interface that is accessed via HTTPS. The local console access to the TOE takes the administrator to the CLI, where the administrative banner is displayed. The banner available at the local console and remote CLI are the same. The banners for the CLI and the GUI are separately configurable.</td></tr>
<tr><td>FTP_ITC.1</td><td>The TOE protects communications with devices to which is sends syslogs, including other iterations of ISE, using TLS. This protects the data from disclosure by encryption and by checksums that verify that data has not been modified.
The TOE also protects communications with external authentication stores in the following manner:
<table>
<tr><td>External Authentication Store</td><td>Protection Mechanism</td></tr>
<tr><td>LDAP Server(s)</td><td>TLS</td></tr>
<tr><td>Active Directory Directory Services (acting as the Secure LDAP server)</td><td>TLS</td></tr>
</table></td></tr>
<tr><td>FTP_TRP.1</td><td>All remote administrative communications take place over a secure encrypted SSHv2 (CLI) session or HTTPS/TLS (web-based GUI) session. Both SSHv2 and HTTPS sessions are protected using AES encryption. The remote users are able to initiate both TLS and SSHv2 communications with the TOE.</td></tr>
</table>

7 ANNEX A: ADDITIONAL INFORMATION

7.1 Key Protection and Zeroization

The following table describes the key zeroization referenced by FCS_CKM.4 provided by the TOE.

Table 18: TOE Key Zeroization

Name	Description	Zeroization
Diffie-Hellman Shared Secret	The value is zeroized after it has been given back to the consuming operation. The value is overwritten by 0's. This key is stored in DRAM.	Automatically after completion of DH exchange, by calling a specific API within the two crypto modules, when module is shutdown, or reinitialized. Overwritten with: 0x00
Diffie Hellman private exponent	The function returns the value to the TOE and then calls the function to perform the zeroization of the generated key pair. These values are automatically zeroized after generation and once the value has been provided back to the actual consumer. This key is stored in DRAM.	Zeroized upon completion of DH exchange, by calling a specific API within the two crypto modules, when module is shutdown, or reinitialized. Overwritten with: 0x00
ISE server certificate	The certificate is used for TLS, HTTPS client connections, secure transport between ISE nodes, and secure connections to authentication stores. The ISE server certificate private key is stored on the local filesystem and in DRAM.	Generation of a new certificate. Overwritten with: 0x00
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents) via API call. This overwrites the key with all 0's. The SSH server host private key is stored on the local filesystem and in DRAM.	Generation of a new key Overwritten with: 0x00
SSH Session Key	The results zeroized by overwriting the values with 0x00. This is done when a session is ended. This key is stored in DRAM.	Automatically when the SSH session is terminated. Overwritten with: 0x00

8 ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 19: References

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004
[NDcPP]	collaborative Protection Profile for Network Devices, Version 1.0, 27 Feb 2015