Forescout

Security Target

ST Version: 1.0
January 23, 2020

Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA, USA 95134

Prepared By:

Booz | Allen | Hamilton

delivering results that endure

Cyber Assurance Testing Laboratory
1100 West St
Laurel MD 20707

Table of Contents

Table of Tables

1 Security Target Introduction

This chapter presents the Security Target (ST) identification information and an overview. An ST contains the Information Technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by the TOE.

1.1 ST Reference

This section provides information needed to identify and control this ST and its Target of Evaluation.

1.2 ST Identification

ST Title: Forescout Security Target
ST Version: 1.0
ST Publication Date: January 23, 2020
ST Author: Booz Allen Hamilton

1.2.1 Document Organization

Chapter 1 of this document provides identifying information for the ST and TOE as well as a brief description of the TOE and its associated TOE type.

Chapter 2 describes the TOE in terms of its physical boundary, logical boundary, exclusions, and dependent Operational Environment components.

Chapter 3 describes the conformance claims made by this ST.

Chapter 4 describes the threats, assumptions, objectives, and organizational security policies that apply to the TOE.

Chapter 5 defines extended Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

Chapter 6 describes the SFRs that are to be implemented by the TSF.

Chapter 7 describes the SARs that will be used to evaluate the TOE.

Chapter 8 provides the TOE Summary Specification, which describes how the SFRs that are defined for the TOE are implemented by the TSF.

1.2.2 Terminology

This section defines the terminology used throughout this ST. The terminology used throughout this ST is defined in Table 1 & 2. These tables are to be used by the reader as a quick reference guide for terminology definitions.

Term	Definition
Administrator, System Administrator, Security Administrator	The class of TOE administrators that are tasked with managing the TOE's functional and security configuration. Embodies those administrators that have access to the CLI and Console.
Connection	One to One simple flows between a network port and a tool port.
Console or Console application	The Forescout Console is a GUI application used for creating NAC, firewall and IPS policies, generating reports, viewing and managing detection information, and managing Forescout Appliances.
Endpoint	A Network Host discovered by the Forescout platform, for example desktop, laptop, server, etc.
Enterprise Manager	A Forescout platform configured to manage multiple Appliances distributed across the network.
Local CLI	When the TOE's command line interface (CLI) is accessed locally with a physical connection to the TOE using the serial port and a terminal emulator that is compatible with serial communications is referred to as the local console.
Plugins	Functionality enhancement modules that can be incorporated into the Forescout platform. Plugins enable deeper inspection as well as broader control over network endpoints. Bundled plugins are pre-packaged with the Forescout platform. Other plugins may be available from Forescout or from a third party.
Network Port	Where data arrives into the TOE. The ports which receive copied network data for the TOE.
Remote console	When the TOE's CLI is accessed remotely using SSH is referred to as the remote console

Table 1: Customer Specific Terminology

Term	Definition
Authorized Administrator	The claimed Protection Profile defines an Authorized Administrator role that is authorized to manage the TOE and its data. For the TOE, this is considered to be any user with the 'admin' role.
Security Administrator	Synonymous with Authorized Administrator and System Administrator.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application an Authorized Administrator uses to manage it (web browser, terminal client, etc.).

Table 2: CC Specific Terminology

1.2.3 Acronyms

The acronyms used throughout this ST are defined in Table 3. This table is to be used by the reader as a quick reference guide for acronym definitions.

Acronym	Definition
CC	Common Criteria
CLI	Command-line Interface

CPU	Central Processing Unit
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
RU	Rack Unit
SAR	Security Assurance Requirement
SCP	Secure Copy Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSL	Secure Sockets Layer
SSH	Secure Shell
ST	Security Target
TAP	Test Access Point
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TP	Tool Port
TSF	TOE Security Function
UI	User Interface

Table 3: Acronym Definition

1.2.4 Reference

[1] collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314 [NDcPP]

[2] 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

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003

[5] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004

[6] NIST Special Publication 800-56B Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, August 2009

[7] NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation, December 2001
[8] FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[9] FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008
[10] FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS) March 2012
[11] FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Standard July 2013
[12] FIPS PUB 197 Advanced Encryption Standard November 26, 2001
[13] FIPS PUB 198-1 Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008

1.3 TOE Reference

The TOE is Forescout which is a family of products, which includes the following appliance models:

CT-R, CT-100, CT-1000, CT-2000, CT-4000, CT-10000, CEM-5, CEM-10, CEM-25, CEM-50, CEM-100, CEM-150, and CEM-200, 5110, 5120, 5140, 5160.

Each appliance runs Forescout software version 8.1.

1.4 TOE Overview

The TOE is the Forescout product and is referred to as the Forescout platform or TOE from this point forward. The Forescout platform is used to dynamically identify and evaluate network infrastructure, devices and applications connected to the network, and provide enforcement of Network Access Policy (NAC) and Enterprise Conformance Policies. Forescout's agentless technology discovers, classifies and assesses devices. The Forescout platform interrogates the network infrastructure to discover devices as they connect to the network. After discovering a device, the Forescout platform uses a combination of passive and active methods to classify the device according to its type and ownership. Based on its classification, The Forescout platform then assesses the device security posture and allows organizations to set policies that establish the specific behavior the device is allowed to have while connected to a network.

The Forescout Console application (aka Console) is a separately installed Windows executable which provides an administrator with a graphical user interface to manage the TOE. The Console must be installed on a separate Windows OS host platform. The Console communicates with the TOE via a secure TLS channel.

The TOE also provides a Command Line Interface (CLI) for remote management of the device. To access the CLI an administrator must either be locally connected, via the keyboard/video or the serial port connections or use SSHv2 to establish a secure connection.

The CLI provides lower level configuration of the device such as initial IP address configuration which cannot be done via the Console, and some diagnostic capabilities. The CLI does not provide any OS-level or shell type access to the embedded OS on the TOE.

The following figure depicts the TOE boundary and operational environment:

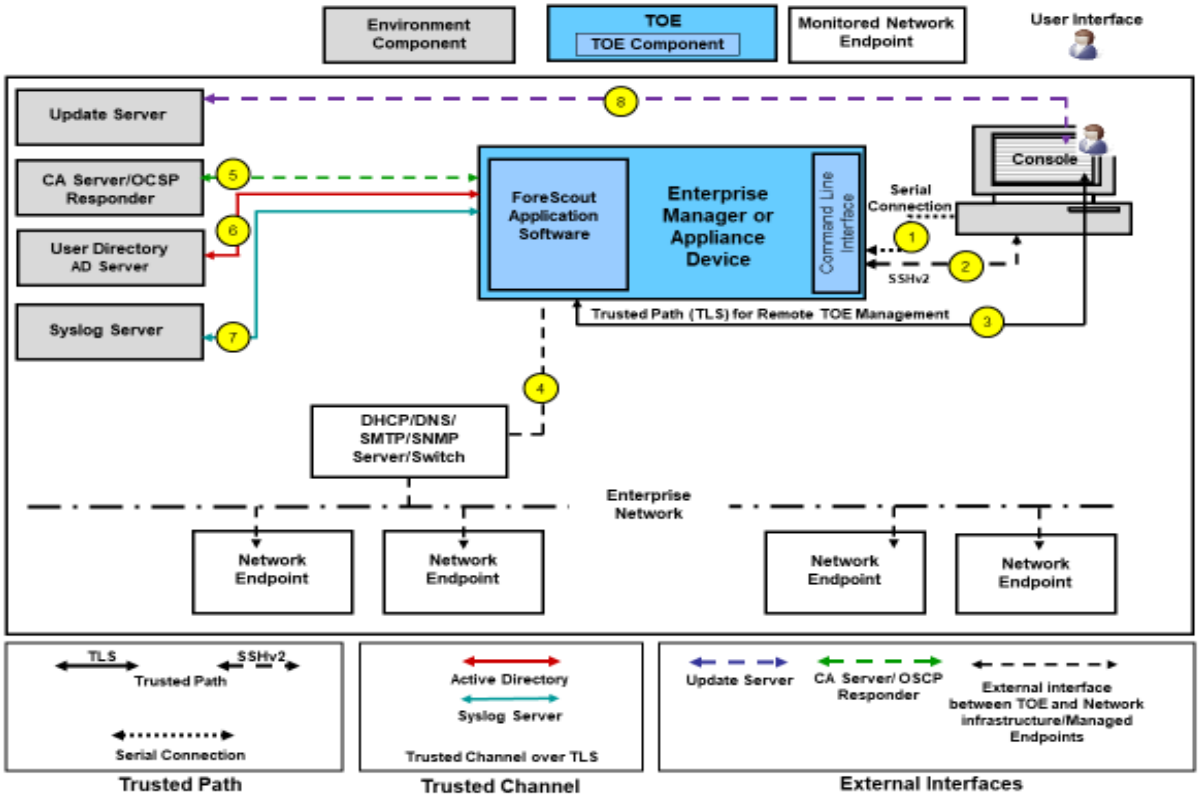

Figure 1: TOE Boundary

As illustrated in Figure 1, the Forescout device and the Console are responsible for all the security functions of the TOE, as scoped by the Protection Profile.

The Forescout platform can be configured as centralized Enterprise Manager (CEM) or as an Appliance. The centralized management functionality does not map to any NDcPP SFRs and is considered beyond the scope of the claimed Protection Profile and was not tested. Therefore, both configurations (CEM and Appliance) of the TOE were tested as standalone entities to ensure that the claimed NDcPP scoped functionality was the same.

1.5 TOE Type

The TOE type for this product is Network Device. The product is a hardware appliance whose primary functionality is related to the handling of network traffic. The NDcPP defines a network device as "a device composed of hardware and software that is connected to the network and has an infrastructure role within the network." Additionally, the NDcPP says that example devices that fit this definition include routers, firewalls, intrusion detection systems, audit servers, and switches.

The TOE is a network device that enables network access control, threat protection, and compliance of the entire enterprise based on network security policies. The TOE type is justified because the TOE provides an infrastructure role in internetworking of different network environments across an enterprise.

2 TOE Description

This section provides a description of the TOE in its evaluated configuration. This includes the physical and logical boundaries of the TOE

2.1 Evaluated Components of the TOE

The following table describes the TOE components in the evaluated configuration:

TOE Components	Hardware Components	Software Version
Forescout Appliances	CT-R, CT-100, CT-1000, CT-2000, CT-4000, CT-10000, CEM-5, CEM-10, CEM-25, CEM-50, CEM-100, CEM-150, and CEM-200, 5110, 5120, 5140, 5160	Forescout v8.1

Table 4: TOE Models

2.2 Components and Applications in the Operational Environment

These components and the functionality they provide are outside the scope of evaluation testing but are needed to support the tested functionality of the TOE. The following table lists components and applications are used in the operational environment for the TOE's evaluated configuration.

Component	Definition

Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. For the TOE to be managed remotely the management workstation is required to have:
	• Non-dedicated machine:
	  o Pentium 3, 1GHz
	  o 2GB memory
	  o 1GB disk space
	• OS running:
	  o Windows 7/8/8.1/10
	  o Windows Server 2008
	  o Linux
	• SSHv2 client installed to access the TOE's CLI
	• Forescout Console application (Console) installed
	
	TCP communications from the Management Workstation to the TOE is secured using:
	• SSH for remote access to the CLI (remote console)
	• TLS for remote access from the Console
	
	The TOE acts as a server for both protocols. Required to support interfaces 1, 2, 3, & 8 as defined in Figure 1 above.
	
	The TOE's CLI can also be accessed locally with a physical connection to the TOE using the keyboard/video or the serial port and must use a terminal emulator that is compatible with serial communications (local console).

Update Server	A general-purpose computer controlled by the vendor that includes a web server and is used to store software update packages that can be retrieved by product customers

	using HTTPS/TLS enabled browser or Console. The host of the Forescout Console provides the secure channel and not the TOE. Therefore, HTTPS is not declared in this ST. The Forescout device does not automatically download or update itself nor does it connect to the update server directly. The TOE receives the update from the Forescout Console. Required to support interface 8 as defined in Figure 1 above and testing for trusted updates.
Certificate Authority (CA) Server/Online Certificate Status Protocol (OCSP) Responder	Certificate authority servers can manage certificate enrollment requests from customers and are able to issue and revoke digital certificates. CA Servers are built to address the identity management requirements. Sending a request to a CA server is usually performed using Simple Certificate Enrollment Protocol (SCEP) over HTTP or Enrollment over Secure Transport (EST) RFC7030 using TLS. An OCSP responder (a server typically run by the certificate issuer) may return a signed response signifying that the certificate specified in the request is 'good', 'revoked', or 'unknown'. If the OCSP responder cannot process the request, it may return an error code. Communications are based on HTTP protocol where the TOE is the client. Required to support interface 5 as defined in Figure 1 above.
Active Directory Server	A system that is capable of receiving authentication requests using LDAP over TLS and validating these requests against identity and credential data that is defined in an LDAP directory. The TOE is the TLS client for this communication. Required to support interface 6 as defined in Figure 1 above.
Syslog Server	The TOE connects to a Syslog Server to send Syslog messages for remote storage via TLS connection where the TOE is the TLS client. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes. Required to support interface 7 as defined in Figure 1 above.
Network Infrastructure	The network infrastructure contains components such as routers, switches, DNS server, etc. Figure 1 identifies these interfaces as a single interface. Interface 4 represents the additional operational network infrastructure required for support. These components are out of scope of the evaluation.

Table 5: Supporting Components in the Operational Environment

2.3 Excluded from the TOE

The following TOE functionality, components, and/or applications are not included in the evaluated configuration. They provide no added security related functionality for the evaluated product. They are separated into three categories: not installed, installed but requires a separate license, and installed but not part of the TSF.

2.3.1 Not Installed

There are no components, applications, and/or functionality that are not installed.

2.3.2 Installed but Requires a Separate License

There are no excluded components, applications, and or functionality that are installed and require a separate license for activation.

2.3.3 Installed But Not Part of the TSF

This section contains functionality that is part of the purchased product but is not part of the TSF relevant functionality that is being evaluated as the TOE based on the Protection Profile.

- **Web Portals** – The different Web Portals provide functionality that allows TOE users, through a local browser or the Console, to view descriptive information such as trend information, vulnerabilities, and network inventory. The Web Portals contain no remote or local security management functionality. They can only provide read-only descriptive information in a dashboard display or that can be incorporated into customized report using the Console. Since the Web Portal interfaces do not have any administrative functionality or any functionality that can be mapped to the NDcPP, they are considered beyond the scope of the claimed Protection Profile.
- **Hierarchical Functionality/Trusted Appliance Interface –** This interface is for a Forescout platform configured as an Enterprise Manager to communicate with another instantiation of the TOE configured as a Forescout Appliance (not an Enterprise Manager) for creating a hierarchical monitoring of a distributed Enterprise network. TLS communications for this interface uses a preconfigured vendor certificate. This interface is not used for remote or local administration. Functionality and Data flow between the two devices does not map to any NDcPP SFRs and is considered beyond the scope of the claimed Protection Profile.
- **Host Scanning –** This functionality allows the TOE to collect vulnerability data and the data used to enforce network access control policies from the network. This functionality is beyond the scope of the claimed Protection Profile.
- **Network Monitor –** This functionality allows the TOE to monitor and track network traffic. This functionality is beyond the scope of the claimed Protection Profile.
- **Network Response –** This functionality allows the TOE to send responses back into the protected network. This functionality is beyond the scope of the claimed Protection Profile.
- **HTTP Redirection –** This functionality allows the TOE to send HTTP (or HTTPS) formatted communications (Web or Intranet) to users on network endpoints. This functionality is beyond the scope of the claimed Protection Profile.
- **SNMP –** The TOE can be configured to use SNMP to communicate with network switches and routers and to receive SNMP traps from network switches and routers. This functionality is beyond the scope of the claimed Protection Profile.
- **SMTP –** The TOE can be configured to use SNMP to send e-mail messages to the administrators or other personnel regarding information of interest. This functionality is beyond the scope of the claimed Protection Profile.

2.4 Physical Boundary

The following table outlines the models and their key differentiators that are part of the evaluation.

System Name	Equipment		
	Software/Firmware	**Hardware Model**	**Component/Configuration**
Forescout: Appliance (CT-) & Enterprise Manager (CEM-)	Forescout v8.1 operating on CentOS 7.5	CT-Remote	1U Desktop
			2 USB 2.0
			1 CPU Intel Celeron J1900 (Bay Trail)
			4x Intel-based 10/100/1000 NIC Ports

Table 6: CT-R Model Rev22

System Name	Equipment		
	Software/Firmware	**Hardware Model**	**Component/Configuration**
Forescout: Appliance (CT-) & Enterprise Manager (CEM-)	Forescout v8.1 operating on CentOS 7.5	CT-100	1U Rack-mount
			3x RAID1 with hot spare
			2x USB 2.0 (back), 2x USB 1.0 (front)
			1 CPU Intel Xeon E5 2609 v3 (Haswell)
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-1000; CEM-05, and CEM-10	1U Rack-mount
			3x RAID1 with hot spare
			2x USB 2.0 (back), 2x USB 1.0 (front)
			1 CPU Intel Xeon E5 2620 v3 (Haswell)
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-2000; CEM-25, and CEM-50	2U Rack-mount
			3x RAID1 with hot spare
			2x USB 2.0 (back), 2x USB 1.0 (front)
			1 CPU Intel Xeon E5 2640 v3 (Haswell)
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-4000; and CEM-100	2U Rack-mount
			3x RAID1 with hot spare
			2x USB 2.0 (back), 2x USB 1.0 (front)
			2 CPU Intel Xeon E5 2640 v3 (Haswell)
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-10000; and CEM-150, CEM-200	2U Rack-mount
			3x RAID1 with hot spare
			2x USB 2.0 (back), 2x USB 1.0 (front)
			2 CPU Intel Xeon E5 2650 v3 (Haswell)
			4 (up to 8)x Intel-based NIC Ethernet Ports

Table 7: CT/CEM Models Rev40

System Name	Equipment		
	Software/Firmware	**Hardware Model**	**Component/Configuration**
Forescout: Appliance (CT-) & Enterprise Manager (CEM-)	Forescout v8.1 operating on CentOS 7.5	CT-100	1U Rack-mount
			3 HDD (RAID1+HS)
			1 USB 2.0 and 1 micro-USB 2.0 (front), 2 USB 3.0 (Rear)
			1 x Xeon Silver 4110 (Skylake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-1000; CEM-05, and CEM-10	1U Rack-mount
			3 HDD (RAID1+HS)

			1 USB 2.0 and 1 micro-USB 2.0 (front), 2 USB 3.0 (Rear)
			1 x Xeon Silver 4110 (Skylake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-2000; CEM-25, and CEM-50	1U Rack-mount
			3 HDD (RAID1+HS)
			1 USB 2.0 and 1 micro-USB 2.0 (front), 2 USB 3.0 (Rear)
			2 x Xeon Silver 4114 (Skylake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-4000; and CEM-100	1U Rack-mount
			3 HDD (RAID1+HS)
			1 USB 2.0 and 1 micro-USB 2.0 (front), 2 USB 3.0 (Rear)
			2 x Xeon Silver 4114 (Skylake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
		CT-10000; and CEM-150, CEM-200	1U Rack-mount
			3 HDD (RAID1+HS)
			1 USB 2.0 and 1 micro-USB 2.0 (front), 2 USB 3.0 (Rear)
			2 x Xeon Gold 5118 (Skylake)
			4 (up to 8)x Intel-based NIC Ethernet Ports

Table 8: CT/CEM Models Rev50

System Name	Equipment		
	Software/Firmware	**Hardware Model**	**Component/Configuration**
Forescout: Appliance (CT-) & Enterprise Manager (CEM-)	Forescout v8.1 operating on CentOS 7.5	5110	1U Desktop
			1 HDD
			2 USB 2.0
			1 CPU Intel Celeron J1900 (Bay Trail)
			4x 10/100/1000 NIC Ports
		5120	1U Rack-mount
			3 HDD (RAID1+HS)
			1 USB 2.0 and 1 micro-USB 2.0 (front), 2 USB 3.0 (Rear)
			1 x Xeon Silver 4110 (Skylake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
		5140	1U Rack-mount
			3 HDD (RAID1+HS)
			1 USB 2.0 and 1 micro-USB 2.0 (front), 2 USB 3.0 (Rear)
			2 x Xeon Silver 4110 (Skylake)
			4 (up to 8)x Intel-based NIC Ethernet Ports
		5160	1U Rack-mount
			3 HDD (RAID1+HS)
			1 USB 2.0 and 1 micro-USB 2.0 (front), 2 USB 3.0 (Rear)
			2 x Xeon Gold 6132 (Skylake)
			4 (up to 8)x Intel-based NIC Ethernet Ports

Table 9: 51xx Models

2.5 Logical Boundary

The TOE is comprised of the following security features that have been scoped by the protection profile:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

2.5.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. The audit logs are stored in an internal database on the TOE's local hard drive. An authorized administrator has the ability to enable/disable the forwarding of events to a syslog server. In the evaluated configuration, the audit data is also securely transmitted to the syslog server using a TLS v1.2 communication channel.

2.5.2 Cryptographic Support

The TOE provides cryptography in support of SSH and TLS (v1.2) trusted communications. Two different cryptography software packages are included with the TOE: Bouncy Castle and OpenSSL. Bouncy Castle uses a hash DRBG and OpenSSL uses a CTR DRBG to provide the random bit generation services with 256 bits of entropy. OpenSSL provides all RSA key generation and is implemented in accordance with FIPS 186-4.Both OpenSSL and Bouncy Castle provide RSA key establishment and is implemented in accordance with RSAES-PKCS1-v1_5. OpenSSL provides Diffie-Hellman group 14 (FFC) key generation is implemented in accordance with RFC 3526, Section 3 and Diffie-Hellman group 14 key establishment is implemented in accordance with RFC 3526, Section 3. Keys are destroyed when no longer used. AES (CBC and GCM), SHA, HMAC, RSA are all used by the TOE for encryption, hashing, message authentication and digital signatures, respectively. The cryptographic implementation has been validated to ensure that the algorithms are appropriately strong for use in trusted communications: OpenSSL: C933 and Bouncy Castle: C944.

2.5.3 Identification and Authentication

The TSF provides a configurable number of maximum consecutive authentication failures that are permitted by a user. Once this number has been met, the account is locked for a configurable time interval or until the Security Administrator manually unlocks the account.

The TOE provides local password authentication as well as providing the ability to securely connect to an Active Directory server for the authentication of users. Communications over this interface is secured using TLS in which the TOE is acting as a client. The TOE enforces X.509 the use of certificates to support authentication for TLS connections. The only function available to an unauthenticated user is the ability to acknowledge a warning banner. Passwords that are maintained by the TSF can be composed of upper case, lower case, numbers and special characters. The Security Administrator can define the password length between 15 and 30 characters.

2.5.4 Security Management

The TOE can be administered locally and remotely and uses role-based access control to prevent unauthorized management. The TOE enforces role-based access control (RBAC) to prevent/allow access to TSF data and functionality. The TOE has one pre-defined role: "Admin". The user permissions for the "Admin" role cannot be modified or customized. A user assigned the "Admin" role is the TOE administrator (Security Administrator) and has access to all Console tools and features. All other users that do not have the full set of administrative permissions are categorized as a "Console User". A Console User's set of permissions are set during creation and can be customized by adding and subtracting specific permissions to allow/disallow the user TOE functionality.

2.5.5 Protection of the TSF

The TOE is expected to ensure the security and integrity of all data that is stored locally and accessed remotely. Passwords are not stored in plaintext. The cryptographic module prevents the unauthorized disclosure of secret cryptographic data. The TOE does not support automatic updates. An administrator has the ability to query the TOE for the currently executing version the TOE software and is required to manually initiate the update process from the Console. The TOE automatically verifies the digital signature of the software update prior to installation. If the digital signature is found to be invalid for any reason the update is not installed. If the signature is deemed invalid, the administrator will be provided a warning banner and allow an administrator to continue with the installation or abort. There is no means for an administrative override to continue the installation if the signature is completely missing. The TOE implements a self-testing mechanism that is automatically executed during the initial start-up and can be manually initiated by an administrator after authentication, to verify the correct operation of product and cryptographic modules. The TOE provides its own time via its internal clock.

2.5.6 TOE Access

The TOE displays a configurable warning banner prior to its use. Inactive sessions will be terminated after an administrator-configurable time period. Users are allowed to terminate their own interactive session. Once a remote session has been terminated the TOE requires the user to re-authenticate to establish a new session. Local and remote sessions are terminated after the administrator configured inactivity time limit is reached.

2.5.7 Trusted Path/Channels

Users can access a CLI for administration functions remotely via SSH (remote console) or a local physical connection (local console) to the TOE. The TOE provides the SSH server functionality. The Console is the main administrator interface, which is running on a separate Windows PC and requires the use of TLS to communicate with the TOE.

The TOE acts as a TLS client to initiate the following secure paths to

- User Authentication (Active Directory)
- Auditing (Syslog)

The TOE acts as a TLS server and receives requests to establish the following secure paths from:

- Forescout Console

3 Conformance Claims

3.1 CC Version

This ST is compliant with Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4 April 2012.

3.2 CC Part 2 Conformance Claims

This ST and Target of Evaluation (TOE) is Part 2 extended to include all applicable NIAP and International interpretations through January 23, 2020.

3.3 CC Part 3 Conformance Claims

This ST and Target of Evaluation (TOE) are conformant to Part 3 to include all applicable NIAP and International interpretations through January 23, 2020.

3.4 PP Claims

This ST claims exact conformance to the following Protection Profiles:

- Collaborative Protection Profile for Network Devices (NDcPP) version 2.0 + Errata 20180314

3.5 Package Claims

The TOE claims exact compliance to the Collaborative Protection Profile for Network Devices (NDcPP) version 2.0 + Errata 20180314, which is conformant with CC Part 3.

The TOE claims following Selection-Based SFRs that are defined in the appendices of the claimed PP:

- FCS_SSHS_EXT.1
- FCS_TLSC_EXT.1
- FCS_TLSS_EXT.1
- FIA_X509_EXT.1/Rev
- FIA_X509_EXT.2
- FIA_X509_EXT.3

The TOE does not claim any Optional SFRs that are defined in the appendices of the claimed PP.

This does not violate the notion of exact conformance because the PP specifically indicates these as allowable options and provides both the ST author and evaluation laboratory with instructions on how these claims are to be documented and evaluated.

3.6 Package Name Conformant or Package Name Augmented

This ST and TOE are in exact conformance with the NDcPP2e.

3.7 Technical Decisions

Technical Decisions that effected the SFR wording have been annotated with a Footnote.

The following list of the NDcPP2e Technical Decisions apply to the TOE because SFR wording, application notes, or assurance activities were modified for SFRs claimed by the TOE:

TD #	Title	Changes				Analysis to this evaluation
		SFR	AA	Notes	NA	Reason
TD0484	NIT Technical Decision for Interactive sessions in FTA_SSL_EXT.1 & FTA_SSL.3			X		No changes to ST
TD0483	NIT Technical Decision for Applicability of FPT_APW_EXT.1	X		X		Changes wording to FPT_APW_EXT.1 and FPT_APW_EXT.2
TD0482	NIT Technical Decision for Identification of usage of cryptographic schemes		X			AA: AGD
TD0481	NIT Technical Decision for FCS_(D)TLSC_EXT.X.2 IP addresses in reference identifiers	X		X		AA: TSS, AGD Test Changes wording to FCS_TLSC_EXT.1.2 not claiming DTLSC
TD0480	NIT Technical Decision for Granularity of audit events		X			AA: Test clarification of general description of audit
TD0478	NIT Technical Decision for Application Notes for FIA_X509_EXT.1 iterations			X		No changes to ST
TD0477	NIT Technical Decision for Clarifying FPT_TUD_EXT.1 Trusted Update		X			AA:Test No changes to ST
TD0475	NIT Technical Decision for Separate traffic consideration for SSH rekey	X	X	X		AA:Test Changes wording to FCS_SSHS_EXT.1.8
TD0453	NIT Technical Decision for Clarify authentication methods SSH clients can use to authenticate SSH se	X			X	Do not claim FCS_SSHC_EXT.1
TD0451	NIT Technical Decision for ITT Comm UUID Reference Identifier				X	Not trying to claim UUID.
TD0450	NIT Technical Decision for RSA-based ciphers and the Server Key Exchange message		X			AA: TSS
TD0447	NIT Technical Decision for Using 'diffie-hellman-group-exchange-sha256' in FCS_SSHC/S_EXT.1.7				X	Not trying to claim diffie-hellman-group-exchange-sha256
TD0425	NIT Technical Decision for Cut-and-paste Error for Guidance AA		X			AA: AGD No changes to ST
TD0423	NIT Technical Decision for Clarification about application of RfI#201726rev2			X		No changes to ST
TD0412	NIT Technical Decision for FCS_SSHS_EXT.1.5 SFR and AA discrepancy		X			AA: Test No changes to ST

TD0411	NIT Technical Decision for FCS_SSHC_EXT.1.5, Test 1 - Server and client side seem to be confused				X	AA: Test Do not claim FCS_SSHC_EXT.1
TD0410	NIT technical decision for Redundant assurance activities associated with FAU_GEN.1		X			TSS: AGD No changes to ST
TD0409	NIT decision for Applicability of FIA_AFL.1 to key-based SSH authentication			X		No changes to ST
TD0408	NIT Technical Decision for local vs. remote administrator accounts	X	X	X		AA: TSS and AGD Changes wording to FIA_UAU_EXT.2.1, FIA_AFL.1.1, and FIA_AFL.1.2
TD0407	NIT Technical Decision for handling Certification of Cloud Deployments				X	Not claiming any cloud platforms
TD0402	NIT Technical Decision for RSA-based FCS_CKM.2 Selection	X	X			AA: Test Changes wording to FCS_CKM.2
TD0401	NIT Technical Decision for Reliance on external servers to meet SFRs			X		No changes to ST
TD0400	NIT Technical Decision for FCS_CKM.2 and elliptic curve-based key establishment			X		No changes to ST
TD0399	NIT Technical Decision for Manual installation of CRL (FIA_X509_EXT.2)				X	Does not claim CRL
TD0398	NIT Technical Decision for FCS_SSH*EXT.1.1 RFCs for AES-CTR	X				Changes to FCS_SSHS_EXT.1.1
TD0397	NIT Technical Decision for Fixing AES-CTR Mode Tests		X		X	AA: Test Do not claim any CTR modes.
TD0396	NIT Technical Decision for FCS_TLSC_EXT.1.1, Test 2		X			AA: Test No changes to ST
TD0395	NIT Technical Decision for Different Handling of TLS1.1 and TLS1.2				X	AA: Test Not claiming mutual authentication
TD0394	NIT Technical Decision for Audit of Management Activities related to Cryptographic Keys			X		No changes to ST
TD0343	NIT Technical Decision for Updating FCS_IPSEC_EXT.1.14 Tests				X	AA: TSS, AGD, and Test Not claiming IPSEC
TD0342	NIT Technical Decision for TLS and DTLS Server Tests		X			AA: Test Not claiming DTLS / Claiming TLSS
TD0341	NIT Technical Decision for TLS wildcard checking			X		AA: Test No changes to ST
TD0340	NIT Technical Decision for Handling of the basicConstraints extension in CA and leaf certificates	X				Changes to FIA_X509_EXT.1.1 text

TD0339	NIT Technical Decision for Making password-based authentication optional in FCS_SSHS_EXT.1.2	X	X	X		AA: TSS and Test Changes to FCS_SSHS_EXT.1.2 text
TD0338	NIT Technical Decision for Access Banner Verification		X			AA: TSS No changes to ST
TD0337	NIT Technical Decision for Selections in FCS_SSH*_EXT.1.6	X	X	X		AA: Test Changes to FCS_SSHS_EXT.1.4 and FCS_SSHS_EXT.1.6 text
TD0336	NIT Technical Decision for Audit requirements for FCS_SSH*_EXT.1.8		X			AA: Test No changes to ST
TD0335	NIT Technical Decision for FCS_DTLS Mandatory Cipher Suites			X		Not claiming DTLSC / Claiming TLSC and TLSS No changes to ST
TD0334	NIT Technical Decision for Testing SSH when password-based authentication is not supported		X		X	Not claiming FCS_SSHC_EXT.1
TD0333	NIT Technical Decision for Applicability of FIA_X509_EXT.3	X	X	X		AA: AGD and Test Changes to FIA_X509_EXT.3.1 text
TD0324	NIT Technical Decision for Correction of section numbers in SD Table 1		X			AA: FSP Evaluation Activities No changes to ST
TD0323	NIT Technical Decision for DTLS server testing - Empty Certificate Authorities list				X	AA: Test Not claiming DTLSC
TD0322	NIT Technical Decision for TLS server testing - Empty Certificate Authorities list		X		X	Not claiming FCS_TLSS_EXT.2
TD0321	Protection of NTP communications				X	No change to ST.
TD0291	NIT technical decision for DH14 and FCS_CKM.1	X	X			AA:Test Change to FCS_CKM.1.1 text
TD0290	NIT technical decision for physical interruption of trusted path/channel.		X			AA: TSS and Test No changes to ST
TD0289	NIT technical decision for FCS_TLSC_EXT.x.1 Test 5e		X			AA: Test No changes to ST
TD0281	NIT Technical Decision for Testing both thresholds for SSH rekey		X			AA: Test clarification No changes to ST
TD0259	NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187	X		X		Changes in selections that could occur were not selected in FCS_SSHS_EXT.1.5 text.
TD0257	NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4		X			AA: Test No changes to ST

TD0256	NIT Technical Decision for Handling of TLS connections with and without mutual authentication		X		X	Not Claiming FCS_TLSC_EXT.2
TD0228	NIT Technical Decision for CA certificates - basicConstraints validation		X			AA: Test No changes to ST

Table 10: Technical Decisions

3.8 Conformance Claim Rationale

The NDcPP states the following: "This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a network device. It provides a minimal set of security requirements expected by all network devices that target the mitigation of a set of defined threats. This baseline set of requirements will be built upon by future cPPs to provide an overall set of security solutions for networks up to carrier and enterprise scale. A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network".

The TOE is a network device composed of hardware and software that is connected to the network. The Forescout appliance is a device that is used to dynamically identify and evaluate network infrastructure, devices and applications connected to the network, and to provide enforcement of Network Access Policy (NAC) and Enterprise Conformance Policies. Therefore, this conformance claim is appropriate.

4 Security Problem Definition

4.1 Threats

This section identifies the threats against the TOE. These threats have been taken from the NDcPP.

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.
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. a 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 includes 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.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

Table 11: TOE Threats

4.2 Organizational Security Policies

This section identifies the organizational security policies which are expected to be implemented by an organization that deploys the TOE. These policies have been taken from the NDcPP.

Policy	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.

Table 12: TOE Organization Security Policies

4.3 Assumptions

The specific conditions listed in this section are assumed to exist in the TOE's Operational Environment. These assumptions have been taken from the NDcPP.

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 a 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 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.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 13: TOE Assumptions

4.4 Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.4.1 TOE Security Objectives

The NDcPP does not define any security objectives for the TOE.

4.4.2 Security Objectives for the Operational Environment

The TOE's operational environment must satisfy the following objectives:

Objective	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	Security Administrators are trusted to follow and apply all guidance documentation 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.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 14: TOE Operational Environment Objectives

4.5 Security Problem Definition Rationale

The assumptions, threats, OSPs, and objectives that are defined in this ST represent the assumptions, threats, OSPs, and objectives that are specified in the Protection Profile to which the TOE claims conformance. The associated mappings of assumptions to environmental objectives, SFRs to TOE objectives, and OSPs and objectives to threats are therefore identical to the mappings that are specified in the claimed Protection Profile.

5 Extended Components Definition

5.1 Extended Security Functional Requirements

The extended Security Functional Requirements that are claimed in this ST are taken directly from the PP to which the ST and TOE claim conformance. These extended components are formally defined in the PP in which their usage is required.

5.2 Extended Security Assurance Requirements

There are no extended Security Assurance Requirements in this ST.

6 Security Functional Requirements

6.1 Conventions

The CC permits four functional component operations—assignment, refinement, selection, and iteration—to be performed on functional requirements. This ST will highlight the operations in the following manner:

- **Assignment:** allows the specification of an identified parameter. Indicated with *italicized* text.
- **Refinement:** allows the addition of details. Indicated with **bold** text.
- **Selection:** allows the specification of one or more elements from a list. Indicated with underlined text.
- **Iteration:** allows a component to be used more than once with varying operations. Indicated with a sequential number in parentheses following the element number of the iterated SFR and/or separated by a "/" with a notation that references the function for which the iteration is used, e.g. "/LocSpace" for an SFR that relates to local storage space

When multiple operations are combined, such as an assignment that is provided as an option within a selection or refinement, a combination of the text formatting is used.

If SFR text is reproduced verbatim from text that was formatted in a claimed PP (such as if the PP's instantiation of the SFR has a refinement or a completed assignment), the formatting is not preserved. This is so that the reader can identify the operations that are performed by the ST author as opposed to the PP author.

6.2 Security Functional Requirements Summary

The following table lists the SFRs claimed by the TOE:

Class Name	Component Identification	Component Name
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User identity association
	FAU_STG_EXT.1	Protected Audit Event Storage
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_TLSC_EXT.1	TLS Client Protocol
	FCS_TLSS_EXT.1	TLS Server Protocol
Identification and Authentication	FIA_AFL.1/CLI	Authentication Failure Management
	FIA_AFL.1/Console	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UIA_EXT.1	User Identification and Authentication

	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
	FIA_X509_EXT.2	X509 Certificate Authentication
	FIA_X509_EXT.3	X509 Certificate Requests
Security Management	FMT_MOF.1/ManualUpdate	Management of security functions behavior
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Trusted Update
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 Banner
Trusted Path /Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1/Admin	Trusted Path

Table 155: Security Functional Requirements for the TOE

6.3 Security Functional Requirements

6.3.1 Class FAU: Security Audit

6.3.1.1 *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 shut-down of the audit functions;

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

c) All administrative actions comprising:

- Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
- Changes to TSF data related to 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]

d) Specifically defined auditable events listed in Table **16**.

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 cPP/ST, information specified in column three of Table **16**.

Requirement	Auditable Event(s)	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.
FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
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_AFL.1/CLI	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address)
FIA_AFL.1/Console	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address)
FIA_PMG_EXT.1	None.	None.
FIA_UAU.7	None.	None.
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	All management activities of TSF data.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	No additional information.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.

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/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 166: Auditable Events

6.3.1.2 *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.

6.3.1.3 *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 [[*invoke a DB purge that will delete oldest entries based on first-in-first-out (FIFO) rules and generate a syslog record for the purge event*]] when the local storage space for audit data is full.

6.3.2 Class FCS: Cryptographic Support

6.3.2.1 *FCS_CKM.1 Cryptographic Key Generation*

FCS_CKM.1.1[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 Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3].

[1] TD0291

6.3.2.2 *FCS_CKM.2 Cryptographic Key Establishment*

FCS_CKM.2.1[2]

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:

[

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"
- Key establishment scheme using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3].

6.3.2.3 *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 [
    - instructs a part of the TSF to destroy the abstraction that represents the key];

that meets the following: No Standard.

6.3.2.4 *FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)*

FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [CBC, GCM] 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, GCM as specified in ISO 19772].

6.3.2.5 *FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)*

FCS_COP.1.1/SigGen

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*]]

[2] TD0402

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]

6.3.2.6 *FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)*

FCS_COP.1.1/Hash

The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits that meet the following: *ISO/IEC 10118-3:2004*.

6.3.2.7 *FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)*

FCS_COP.1.1/KeyedHash

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [*160 bits, 256 bits, 384 bits, 512 bits*] and message digest sizes [160, 256, 384, 512] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".

6.3.2.8 *FCS_RBG_EXT.1 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 [Hash_DRBG (any), CTR_DRBG (AES)].

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*4*] software-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.

6.3.2.9 *FCS_SSHS_EXT.1 SSH Server Protocol*

FCS_SSHS_EXT.1.1[3]

The TSF shall implement the SSH protocol that complies with RFC(s) [4251, 4252, 4253, 6668].

[3] TD0398

FCS_SSHS_EXT.1.2[4]

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 [*32,768*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4[5]

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms*:* [aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, aes256-gcm@openssh.com].

FCS_SSHS_EXT.1.5[6]

The TSF shall ensure that the SSH public-key based authentication implementation uses [ssh-rsa] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6[7]

The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512, implicit] as its data integrity 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 methods used for the SSH protocol.

FCS_SSHS_EXT.1.8[8]

The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

6.3.2.10 *FCS_TLSC_EXT.1 TLS Client Protocol*

FCS_TLSC_EXT.1.1

The TSF shall implement [*TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_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

[4] TD0339
[5] TD0337
[6] TD0259
[7] TD0337
[8] TD0475

- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288]

FCS_TLSC_EXT.1.2[9]

The TSF shall verify that the presented identifier of the following types: [identifiers defined in RFC 6125] are matched to reference identifiers.

FCS_TLSC_EXT.1.3

The TSF shall only establish a trusted channel if the server certificate is valid. If the server certificate is deemed invalid, then the TSF shall [not establish the connection].

FCS_TLSC_EXT.1.4

The TSF shall [not present the Supported Elliptic Curves Extension] in the Client Hello.

6.3.2.11 *FCS_TLSS_EXT.1 TLS Server Protocol*

FCS_TLSS_EXT.1.1

The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:[

- TLS_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_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288].

FCS_TLSS_EXT.1.2

The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [TLS 1.1].

FCS_TLSS_EXT.1.3

The TSF shall [perform RSA key establishment with key size [2048 bits]].

6.3.3 Class FIA: Identification and Authentication

6.3.3.1 *FIA_AFL.1/CLI Authentication Failure Management*

FIA_AFL.1.1[10]

The TSF shall detect when an Administrator configurable positive integer within [*1-5*] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

FIA_AFL.1.2[11]

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending Administrator from successfully establishing remote session using any

[9] TD0481
[10] TD0408
[11] TD0408

authentication method that involves a password until an Administrator defined time period has elapsed].

6.3.3.2 *FIA_AFL.1/Console Authentication Failure Management*

FIA_AFL.1.1[12]

The TSF shall detect when an Administrator configurable positive integer within [*1-5*] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

FIA_AFL.1.2[13]

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until [*a manual unlock of the account*] is taken by an Administrator; prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

6.3.3.3 *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 configurable to [*15*] and [*30*].

6.3.3.4 *FIA_UAU.7 Protected Authentication Feedback*

FIA_UAU.7.1

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

6.3.3.5 *FIA_UAU_EXT.2 Password-based Authentication Mechanism*

FIA_UAU_EXT.2.1[14]

The TSF shall provide a local [password-based, SSH public key-based, certificate-based, [*Active Directory*] authentication mechanism to perform local administrative user authentication.

[12] TD0408
[13] TD0408
[14] TD0408

6.3.3.6 *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.

6.3.3.7 *FIA_X509_EXT.1/Rev X.509 Certificate Validation*

FIA_X509_EXT.1.1/Rev[15]

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

- RFC 5280 certificate validation and certificate path validation supporting a minimum path length of three certificates.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 5280 Section 6.3].
- 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/Rev

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.

[15] TD0340

6.3.3.8 *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 [not accept the certificate].

6.3.3.9 *FIA_X509_EXT.3 X.509 Certificate Requests*

FIA_X509_EXT.3.1[16]

The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name].

FIA_X509_EXT.3.2

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

6.3.4 Class FMT: Security Management

6.3.4.1 *FMT_MOF.1/ManualUpdate Management of security functions behavior*

FMT_MOF.1.1/ManualUpdate

The TSF shall restrict the ability to enable the functions to perform manual updates to Security Administrators.

6.3.4.2 *FMT_MTD.1/CoreData Management of TSF Data*

FMT_MTD.1.1/CoreData

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

6.3.4.3 *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 authentication failure parameters for FIA_AFL.1;

[16] TD0333

- [
  - Ability to configure the cryptographic functionality;
  - Ability to re-enable an Administrator account;
  - Ability to set the time which is used for time-stamps;

  ]

6.3.4.4 *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.

6.3.5 Class FPT: Protection of the TSF

6.3.5.1 *FPT_APW_EXT.1 Protection of Administrator Passwords*

FPT_APW_EXT.1.1[17]

The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2[18]

The TSF shall prevent the reading of plaintext administrative passwords.

6.3.5.2 *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.

6.3.5.3 *FPT_STM_EXT.1 Reliable Time Stamps*

FPT_STM_EXT.1.1

The TSF shall be able to provide reliable time stamps for its own use.

[17] TD0483
[18] TD0483

FPT_STM_EXT.1.2

The TSF shall [allow the Security Administrator to set the time].

6.3.5.4 *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), at the request of the authorised user] to demonstrate the correct operation of the TSF: [*Specifically defined in Table 17*].

#	Validation	Component
1.	HMAC + Built-in Crypto Self-test	Kernel
2.	Built-in RPM Verification	Core OS and packages (including OpenSSH)
3.	HMAC verified against fipshmac	Fipscheck utility
4.	Fipscheck (including OpenSSL self-check)	Crypto: OpenSSL
5.	Built-in RPM Verification	OpenSSL rpm package
6.	Built-in crypto package self-test (KAT)	Crypto: Bouncy Castle
7.	SHA-256 verified against last known or stored hash.	Core Platform and plugin installation packages and extracted files.
8.	Running kernel version compared to version defined in grub;	System current state vs system configuration

Table 17: Self-Test List

6.3.5.5 *FPT_TUD_EXT.1 Trusted Update*

FPT_TUD_EXT.1.1

The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [no other TOE firmware/software version].

FPT_TUD_EXT.1.2

The TSF shall provide Security Administrators the ability to manually initiate updates to 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.

6.3.6 Class FTA: TOE Access

6.3.6.1 *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.

6.3.6.2 *FTA_SSL.3 TSF-initiated Termination*

FTA_SSL.3.1

The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

6.3.6.3 *FTA_SSL.4 User-initiated Termination*

FTA_SSL.4.1

The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

6.3.6.4 *FTA_TAB.1 Default TOE Access Banner*

FTA_TAB.1.1

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.

6.3.7 Class FTP: Trusted Path/Channels

6.3.7.1 *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 [*export audit, authentication decision*].

6.3.7.2 *FTP_TRP.1/Admin Trusted Path*

FTP_TRP.1.1/Admin

The TSF shall be capable of using [SSH, TLS] 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 provides 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 administration actions.

6.4 Statement of Security Functional Requirements Consistency

The Security Functional Requirements included in the ST represent all required SFRs specified in the PPs against which exact conformance is claimed and a subset of the optional SFRs. All hierarchical relationships, dependencies, and unfulfilled dependency rationales in the ST are considered to be identical to those that are defined in the claimed PP.

7 Security Assurance Requirements

This section identifies the Security Assurance Requirements (SARs) that are claimed for the TOE. The SARs which are claimed are in exact conformance with the NDcPP.

7.1 Class ADV: Development

7.1.1 Basic Functional Specification (ADV_FSP.1)

7.1.1.1 *Developer action elements:*

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

The developer shall provide a tracing from the functional specification to the SFRs.

7.1.1.2 *Content and presentation elements:*

ADV_FSP.1.1C

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

7.1.1.3 *Evaluator action elements:*

ADV_ FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_ FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

7.2 Class AGD: Guidance Documentation

7.2.1 Operational User Guidance (AGD_OPE.1)

7.2.1.1 *Developer action elements:*

AGD_OPE.1.1D

The developer shall provide operational user guidance.

7.2.1.2 *Content and presentation elements:*

AGD_OPE.1.1C

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C

The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

7.2.1.3 *Evaluator action elements:*

AGD_OPE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.2.1.4 *Developer action elements:*

7.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

7.2.2.1 *Content and presentation elements:*

AGD_ PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_ PRE.1.2C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

7.2.2.2 *Evaluator action elements:*

AGD_ PRE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_ PRE.1.2E

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

7.3 Class ALC: Life Cycle Support

7.3.1 Labeling of the TOE (ALC_CMC.1)

7.3.1.1 *Developer action elements:*

ALC_CMC.1.1D

The developer shall provide the TOE and a reference for the TOE.

7.3.1.2 *Content and presentation elements:*

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

7.3.1.3 *Evaluator action elements:*

ALC_CMC.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.3.2 TOE CM Coverage (ALC_CMS.1)

7.3.2.1 *Developer action elements:*

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

7.3.2.2 *Content and presentation elements:*

ALC_CMS.1.1C

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

7.3.2.3 *Evaluator action elements:*

ALC_CMS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

7.4 Class ATE: Tests

7.4.1 Independent Testing - Conformance (ATE_IND.1)

7.4.1.1 *Developer action elements:*

ATE_IND.1.1D

The developer shall provide the TOE for testing.

7.4.1.2 *Content and presentation elements:*

ATE_IND.1.1C

The TOE shall be suitable for testing.

7.4.1.3 *Evaluator action elements:*

ATE_IND.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

7.5 Class AVA: Vulnerability Assessment

7.5.1 Vulnerability Survey (AVA_VAN.1)

7.5.1.1 *Developer action elements:*

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

7.5.1.2 *Content and presentation elements:*

AVA_VAN.1.1C

The TOE shall be suitable for testing.

7.5.1.3 *Evaluator action elements:*

AVA_VAN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

8 TOE Summary Specification

The following sections identify the security functions of the TOE and describe how the TSF meets each claimed SFR. They include Security Audit, Cryptographic Support, Identification and Authentication, Security Management, Protection of the TSF, TOE Access and Trusted Path / Channels.

8.1 Security Audit

8.1.1 FAU_GEN.1 and FAU GEN.2

The TOE has the mechanisms to automatically generate audit records based on the behavior that occurs within the TSF. The TOE generates audit records for all administrative functions including Login/Logout, security related changes, resetting of passwords, starting and stopping the TOE (equivalent to starting and stopping audit), and certificate management. Additionally, Table 16 identifies the audit records that are inclusive to the PP evaluation scoping. The TOE records the date and time, type of event, subject identity (identity of the user associated with each audited event that occurred due to a user action), and the outcome in the audit record. The TOE associates each auditable event with the identity of the user that caused the event. Fore a fill list of the audit events samples that are generated by the TOE, please refer to the Supplemental Administrative Guidance Document (AGD).

The TOE application layer maintains two separate log files in an internal database to record all the records needed to satisfy this requirement as scoped by the PP. The host OS also maintains an audit log (OS log) that is stored locally on the hard drive. All OS log records are incorporated into the appropriate application layer logs based on the type of event. The two application layer logs are as follows:

- **User Audit Trail**
  The User Audit Trail records information concerning TOE user activity for both CLI (OS log) and Console interface, for example: administrative changes to the security configuration of the TOE or updated/resetting of user passwords. The logs give additional information about the activity, such as the date of the activity and the IP address from which it was carried out.
- **System Event Log**
  The System Event Log records information about system activity, for example: successful and failed administrator authentication attempts, startup and shutdown of TOE or services, cryptographic key generation and destruction, and OS events. The startup and shutdown of the TOE's audit functionality is synonymous with the startup and shutdown of the TOE.

The following is an example audit record for the Generating/import of, changing, or deleting of cryptographic keys:

Generating/import of, changing, or deleting of cryptographic keys	Feb 7 09:08:07 FS3 FS3[17471]: User admin changed Configuration. Details: Change trusted certificates configuration definition to Added Fingerprint 'c4650e925d4334c895f3bd163884886a9d9d0116', Issued To 'intermediate02.cctl.com', Issued By 'Intermediate01.cctl.com', enabled, Trusted By 'All' on 'All'

8.1.2 FAU_STG_EXT.1

The TSF provides the ability for an administrator to enable/disable the near real-time forwarding of the audit trail to an external syslog server in the operational environment. The forwarding of the audit trail to a syslog server is mandated for compliance to the NDcPP. Once enabled, the generated audit is first saved locally in the internal database and then the TOE will securely transmit audit data to the Operational Environment syslog server without administrator intervention via a TLS channel.

Application layer audit events are stored in the TOE database (DB). The TOE runs an automatic DB purge function to prevent audit logs from filling up the internal database and hard drive to capacity. The DB, as part of the installation, determines a maximum size based on hard drive availability. This predefined and configurable threshold is used to trigger the DB purge function. The DB purge function is initiated when 75 percent of this predefined and a configurable threshold is exceeded. When the DB threshold is exceeded, the DB purge function deletes entries in a FIFO (oldest events deleted first) fashion. The DB purge function causes a syslog event to be sent by the TOE.

The TOE also takes into consideration the storage needed for the OS log files when preventing the hard drive being filled to capacity. The TOE provides an administrator with the ability to define a maximum size for the OS log file and the number of OS log files (current plus historical) saved at the OS level.

When the OS log file reaches the administratively defined maximum size, the log file is closed and renamed sequentially (i.e. OSlog.1, OSlog.2). This means that if an administrator configures the TOE to keep the maximum setting of 5 log files then there will be 5 OS logs maintained on the system (the currently opened and 4 historical).

The administrator can configure the maximum size of OS log files to 50 MB. This configuration setting applies to all OS log files (current and historical). Therefore, with a maximum setting of 5 audit logs and a maximum setting file size of 50MB each would result in 5*50MB= 250MB of total audit space required for the OS logs. Once the number of log files reaches its configured maximum amount, the oldest log file is automatically deleted, and the remaining log files roll over in order to allow the new file to be created for the new audit records.

The TOE provides a means to review all of the audit records via the Console interface. The TOE does not provide a means for any user to manually delete or manipulate the audit logs stored at the OS level or those in the internal DB. The management interfaces (Console or CLI) do not allow the audit records to be modified or deleted. The audit functionality starts automatically with the TOE and cannot be disabled by any means.

8.2 Cryptographic Support

The TOE implements two different cryptographic modules: OpenSSL and Bouncy Castle. Both modules include algorithms that are certified under the following consolidated CAVP certificates:

a) OpenSSL FIPS library under CAVP Cert # C933

b) BC-FJA (Bouncy Castle FIPS Java API) Software Version 1.0.0 under CAVP Cert # C944

The following tables contain the CAVP algorithm certificates for the two cryptographic modules implemented in the TOE:

SFR	Algorithm/Protocol	OpenSSL CAVP Cert #
FCS_CKM.1	RSA FIPS 186-4 Key Generation	C933
	FFC using Diffie-Hellman group 14, RFC 3526 Section 3	N/A
FCS_CKM.2	RSA Key Establishment RSAES-PKCS-v1_5	Vendor Affirmation
	Diffie-Hellman group 14 Key Establishment RFC 3526 Section 3	N/A
FCS_COP.1/DataEncryption	AES CBC and GCM Mode, 128 and 256 bits	C933
FCS_COP.1/SigGen	RSA FIPS 186-4 Signature Services 2048 bits	C933
FCS_COP.1/Hash	SHS: SHA-1, SHA-256, SHA-384, and SHA-512	C933
FCS_COP.1/KeyedHash	HMAC-SHA-1, HMAC-SHA-256, HMAC-384, HMAC-SHA-512	C933
FCS_RBG_EXT.1	CTR DRBG	C933

Table 18: Cryptographic Algorithm Table for OpenSSL

SFR	Algorithm/Protocol	Forescout CAVP Cert #
FCS_CKM.1	RSA FIPS 186-4 Key Generation	N/A
FCS_CKM.2	RSA Key Establishment RSAES-PKCS-v1_5	Vendor Affirmation
FCS_COP.1/DataEncryption	AES CBC and GCM Mode, 128 and 256 bits	C944
FCS_COP.1/SigGen	RSA FIPS 186-4 Signature Generation and Signature Verification 2048 bits	C944
FCS_COP.1/Hash	SHS: SHA-1, SHA-256, and SHA-384	C944
FCS_COP.1/KeyedHash	HMAC-SHA-1, HMAC-SHA-256, HMAC-384	C944
FCS_RBG_EXT.1	Hash DRBG	C944

Table 19: Cryptographic Algorithm Table for Bouncy Castle

8.2.1 FCS_CKM.1

The TOE implements a FIPS PUB 186-4 conformant key generation mechanism for RSA key generation schemes for establishing TLS connections. Specifically, the TOE complies with the FIPS 186-4 (Digital Signature Standard (DSS) Appendix B.3). This is used to generate the RSA key pairs with a modulus of at least 2048 bits which has an equivalent key strength of 112 bits. See Tables 18 & 19 Cryptographic Algorithm Table for certification numbers.

Only the OpenSSL cryptographic module is used for key generation. The Bouncy Castle cryptographic module is not used for key generation.

In addition, the TOE implements FFC schemes using Diffie-Hellman group 14 that meets RFC 3526, Section 3. This is used to generate the keys of size 2048 bits for diffie-hellman-group14-sha1. DH group 14 support is provided by the OpenSSL cryptographic module.

8.2.2 FCS_CKM.2

The TOE implements RSA key establishment, conformant to RSAES-PKCS1-v1_5. The TOE complies with section 7.2 of RFC 8017, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography

Specifications Version 2.1 and all subsections regarding RSA key pair generation and key establishment in RSAES-PKCS1-v1_5. The TOE uses the OpenSSL cryptographic module to generate RSA key pairs with a modulus of at least 2048 bits which has an equivalent key strength of 112 bits. The RSA key establishment is used for TLS communications for remote administration using the Console, exporting audit to audit server, and authentication requests to external authentication server.

In addition, the TOE implements a key establishment scheme using Diffie-Hellman group 14 that meets RFC 3526, Section 3. DH group 14 support is provided by the OpenSSL cryptographic module. The TSF uses Diffie-Hellman-group14-SHA1 and is used for SSH communication establishment in support of remote CLI administration. The Diffie-Hellman group 14 is implemented by using the KexAlgorithms parameter as specified in RFC 3526 Section 3. SSH is also forced to only work with DH group 14. This is hardcoded with no ability for an administrator to modify the settings.

Below is a table that summarizes which cryptographic module is supporting which claimed interface.

OE Component	Definition of Communication (protocol, client/server, crypto module)
Management Workstation	Communications are secured using TLS where the TOE is the Server. TOE crypto required to support interface 3 as defined in Figure 1 above. Key Generation Crypto Module: OpenSSL RSA Key establishment and encryption for TLS: Bouncy Castle
	Communications are secured using SSH where the TOE is the Server TOE crypto required to support interface 2 as defined in Figure 1 above. Key Generation Crypto Module: OpenSSL Diffie-Helman Group 14 Key establishment and encryption for SSH: OpenSSL
Active Directory Server	Communications are secured using TLS where the TOE is the client. TOE crypto required to support interface 6 as defined in Figure 1 above. Key Generation Crypto Module: OpenSSL RSA Key establishment and encryption for TLS: OpenSSL
Syslog Server	Communications are secured using TLS where the TOE is the client. TOE crypto required to support interface 7 as defined in Figure 1 above. Key Generation Crypto Module: OpenSSL RSA Key establishment and encryption for TLS: OpenSSL

Table 20: Identification of Crypto Module Supporting Secured Communication Channel

8.2.3 FCS_CKM.4

The following table describes what keys were used, where they are stored, and also how they are destroyed. There are no known instances where key destruction does not happen as defined

Name	Origin	Store	Zeroization / Destruction
Diffie-Hellman Shared Secret	SSH Server / client applications	RAM	Destroyed by a single direct overwrite consisting of zeroes (0x00)*. After overwriting, the TSF reads the memory to verify the key has been destroyed. If the read-verify fails, the process is repeated. The key is zeroized immediately after it is no longer needed and when the TOE is

			shutdown or reinitialized. Automatically zeroized after DH exchange.
Diffie-Hellman private exponent	SSH Server / client applications	RAM	Destroyed by a single direct overwrite consisting of zeroes (0x00)*. After overwriting, the TSF reads the memory to verify the key has been destroyed. If the read-verify fails, the process is repeated. The key is zeroized immediately after it is no longer needed and when the TOE is shutdown or reinitialized. Automatically zeroized after DH exchange
SSH session key	SSH Server / client applications	RAM	Destroyed by a single direct overwrite consisting of zeroes (0x00)*. After overwriting, the TSF reads the memory to verify the key has been destroyed. If the read-verify fails, the process is repeated. The key is zeroized immediately after it is no longer needed and when the TOE is shutdown or reinitialized. Automatic zeroized after SSH session is terminated.
SSH Server Host Private Key	Generated on platform during initial setup of device.	Filesystem	Filesystem: Generation of a new certificate will only be accomplished during a reinstallation of the product where all files would be overwritten which would in effect also destroy the abstraction that represented the key.
TLS Server Host Certificate Private Key	Generated on platform (OpenSSL) during initial setup or imported after installation. Syslog TLS Communications for syslog, AD Bouncy Castle TLS Communication for Console	RAM and Filesystem	RAM: The Server Certificate's private key is destroyed by a single direct overwrite consisting of zeroes (0x00)*. After overwriting, the TSF reads the memory to verify the key has been destroyed. If the read-verify fails, the process is repeated. The key is zeroized immediately after it is no longer needed and when the TOE is shutdown or reinitialized. Filesystem: Private key is deleted when generation of a new certificate are imported or when certificates are removed. The TOE will invoke an interface, provided by a part of the TSF, that instructs a the TSF to destroy the abstraction that represents the key (i.e. delete the resource).

Table 21: Crypto key destruction table

*OpenSSL: Cleanse () and Bouncy Castle: JVM garbage collection APIs that perform zeroization

8.2.4 FCS_COP.1/DataEncryption

The TOE performs encryption and decryption using the AES algorithm in CBC and GCM modes with key sizes of 128 and 256 bits. The AES algorithm meets ISO 18033-3, CBC meets ISO 10116 and GCM meets ISO 19772. The TOE's AES implementation is validated under CAVP. See Tables 18 & 19 Cryptographic Algorithm Table for certification numbers.

This is applicable to both cryptographic modules being implemented.

8.2.5 FCS_COP.1/SigGen

The TOE performs digital signature services generation and verification in accordance with RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) 2048 bits or greater. The RSA schemes are in accordance with 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. The TOE's RSA implementation is validated under CAVP. See Tables 18 & 19 Cryptographic Algorithm Table for certification numbers.

This is applicable to both cryptographic modules being implemented.

8.2.6 FCS_COP.1/Hash

The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512* as specified in ISO/IEC 10118-3:2004 (FIPS PUB 180-4). The TOE's SHS implementation is validated under CAVP. See Tables 18 & 19 Cryptographic Algorithm Table for certification numbers. This is applicable to both cryptographic modules being implemented. The hashing function is used to support password hashing of all passwords stored on the TOE (FPT_APW_EXT.1), Trusted updates digital signature verification (FPT_TUD_EXT.1), and TSF self-testing hash value check verification (FPT_TST_EXT.1).

*Only the OpenSSL cryptographic module provides the SHA-512 hashing support. Meaning:

- OpenSSL supports: SHA-1, SHA-256, SHA-384, and SHA-512
- Bouncy Castle supports: SHA-1, SHA-256, and SHA-384

8.2.7 FCS_COP.1/KeyedHash

The TOE provides keyed-hashing message authentication services that meet ISO/IEC 9797-2:2011 (FIPS PUB 198-1, and FIPS PUB 180-4), Section 7 "MAC Algorithm 2". The TOE supports the following:

- HMAC-SHA-1 [key-size: 160 bits, digest size: 160 bits, block size: 512 bits, MAC lengths: 160 bits] for SSH and TLS communication support
- HMAC-SHA-256 [key-size: 256 bits, digest size: 256 bits, block size: 512 bits, MAC lengths: 256 bits] for SSH and TLS communication support
- HMAC-SHA-384 [key-size: 384 bits, digest size: 384 bits, block size: 1024 bits, MAC lengths: 384 bits] for TLS communication support only
- HMAC-SHA-512* [key-size: 512 bits, digest size: 512 bits, block size: 1024 bits, MAC lengths: 512 bits] for SSH communication support only

The TOE's HMAC implementation is validated under CAVP. See Tables 18 & 19 Cryptographic Algorithm Table for certification numbers.

*Only the OpenSSL cryptographic module provides HMAC-SHA-512 keyed-hashing message authentication. Meaning:

- OpenSSL supports: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512
- Bouncy Castle supports: HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-384

.

8.2.8 FCS_RBG_EXT.1

The TOE implementation of Bouncy Castle uses a hash deterministic random bit generator (Hash_DRBG). The TOE implementation of OpenSSL uses a counter mode random be generator (CTR DRBG). Both DRBG used by the TOE are in accordance with ISO/IEC 18031:2011. There is no ability to specify the use of an alternative DRBG. The different TOE models uniformly provide four software-based noise-based entropy sources as described in the proprietary entropy specification. The amount of entropy that is collected is based on the function that the DRBG is being used for. In all cases, this amount is greater than or equal to the security strength of the data that is being output. For example, a 256-bit AES key generation operation will collect at least 256 bits of entropy before the DRBG is invoked. The largest AES key generation operation supported is 2048-bit.

The Bouncy Castle and OpenSSL module collect entropy from /dev/random, which is a blocking entropy source. The /dev/random entropy pools are protected by being in kernel memory and are not accessible from user space. The entropy source is described in greater detail in the proprietary Entropy Assessment Report.

Forescout currently relies on kernel modules to gather and output entropy for our random uses:

- Interrupt events - the timestamp of the event, the IRQ number and interrupt flags are used
- Disk events - the timestamp of a disk operation completion event is used
- Keyboard event - the timestamp of a keyboard press/release event and the key code are used
- CPU cycles event – the output of the 32-bit counter that measures CPU cycles

The TOE's DRBG implementation is validated under CAVP. See Tables 18 & 19 Cryptographic Algorithm Table for certification numbers.

8.2.9 FCS_SSHS_EXT.1

The TOE acts as an SSHv2 server for remote CLI sessions that complies with RFCs 4251, 4252, 4253, and 6668. The TOE implementation of SSH supports public key-based and password-based authentication. SSH is used for remote administrators to connect securely to the TOE for CLI connections. The SSH implementation will detect all large packets greater than 32,768 bytes and drop accordingly. Additionally, the TSF enforces the connection to be rekeyed after no longer than one hour, and no more than one gigabyte of transmitted data, whichever threshold is reached first. These parameters are not configurable.

The TOE's implementation of SSHv2 only supports:

- aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, aes256-gcm@openssh.com for its encryption algorithms
- ssh-rsa, as its only public key algorithms.

- hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512, and implicit for data integrity
- diffie-hellman-group14-sha1 for key exchange method in accordance with RFC 3526 Section 3.

OpenSSL cryptographic module provides all cryptographic support required for SSH communication.

8.2.10 **FCS_TLSC_EXT.1**

The TOE when acting as a TLS client will only support TLSv1.2 protocols to connect and secure the following trusted channels:

- performing authentication requests with the AD Server,
- audit data transfer

Mutual authentication is not being claimed.

The following ciphersuites are used for the evaluated configuration:

- TLS_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_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288

The TOE does not support elliptic curves.

The TOE will only establish a trusted channel if the peer certificate is valid. The TSF shall verify the presented identifier matches the reference identifier according to RFC 6125. The Common Name and Subject Alternative Name (DNS Name only) are the only reference identifiers in the certificate that is part of that validation. The TOE will only support a wildcard in the left-most label (e.g. *.example.com). All other usages of a wildcard will cause a failure in the connection. The TOE does not support URI, IP addresses or service name reference identifiers or pinned certificates.

OpenSSL provides the cryptographic support for key establishment and encryption for these TLS channels.

8.2.11 **FCS_TLSS_EXT.1**

The TOE, when acting as a TLS server, will only support TLSv1.2 protocols to connect and secure the following trusted channels:

- Console remotely connecting to the TOE for remote management

The TOE will deny connections from a client requesting SSL 2.0, SSL 3.0, TLSv1.0, TLSv1.1 protocol versions.

The following ciphersuites are used for the evaluated configuration:

- TLS_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_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288

The TSF generates key establishment parameters using RSA with key size of 2048 bits.
Elliptic Curves are not supported, and mutual authentication is not being claimed.

Bouncy Castle provides the cryptographic support for key establishment and encryption TSL channel.

8.3 Identification and Authentication

8.3.1 FIA_AFL.1/CLI and FIA_AFL.1/Console

The TSF provides a configurable counter for consecutive failed authentication attempts that will lock a user account when the failure counter threshold is reached.

For CLI user accounts that are locked: A user with a locked account cannot login to either the CLI or local console until a configurable time limit set by the Security Administrator has elapsed. This prevents a total lockout of the system.

For Console user accounts that are locked: A user with a locked account cannot login into the Console application until a Security Administrator manually unlocks the account or a configurable time limit set by the Security Administrator has elapsed, whichever comes first.

A valid login that happens prior to the failure counter reaching its threshold will reset the counter to zero.

The Security Administrator is able to configure the number of failed attempts before the lockout of the offending account occurs. This can be set at a minimum of 1 and maximum of 5 consecutive failed attempts. The default is always set at 3 consecutive failed attempts. The Security Administrator is also able to define a time period when the account will automatically unlock. The default for this setting is 30 minutes and can be configured between 5 minutes and indefinitely. This timer setting applies to both CLI and Console user accounts.

8.3.2 FIA_PMG_EXT.1

The TOE supports the ability for the Security Administrator to set the minimum password length to 15 characters or greater with a maximum of 30 characters. Passwords can be composed of any combination of upper- and lower-case letters, numbers and special characters. The accepted special characters include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")".

8.3.3 FIA_UAU.7

When authenticating to the TOE with a local physical connection (local console) to access the CLI, the password is obscured by suppressing the echo of keystrokes to the screen. No indication of progress is provided while typing in a password. Also, in the case of an invalid username or password, the TOE does not reveal any information about the invalid component.

8.3.4 FIA_UAU_EXT.2 and FIA_UIA_EXT.1

The warning banner text can be configured by the administrator. The display and acknowledgement of this banner is the only TOE functionality that is available to an unauthenticated user.

When connecting to the TOE remotely using an SSH client (remote console) or using a local physical connection (local console) to gain access to the CLI, the TOE displays the pre-authentication warning banner. Users are authenticated using a native username/password credential authentication mechanism for local physical connections and SSH connections. SSH connections also support public key-based authentication.

When connecting to the TOE remotely using the Console application, which establishes a TLS connection, the TOE displays the pre-authentication warning banner is displayed. The TOE can be configured to request an authentication decision from an Active Directory server or use the native username/password credential authentication mechanism for users connecting to the TOE using the Console.

Access is only granted once the user provides a valid username/password that is verified using Active Directory or native username/password credential authentication mechanism.

8.3.5 FIA_X509_EXT.1/Rev, FIA_X509_EXT.2, and FIA_X509_EXT.3

The TOE uses X.509v3 certificates to support authentication for TLS connections to external IT entities in accordance with RFC 5280. When the TSF cannot determine the validity of a certificate, the TSF will not accept the certificate and not establish a connection or accept the certificate and establish the connection. The TSF does not provide a mechanism to override the validation decision.

The TSF determines the validity of certificates by ensuring that the certificate and the certificate path is valid in accordance with RFC 5280. In addition:

- 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
- 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 5280 Section 6.3.
- When the TSF cannot establish a connection to determine the validity of a certificate the TSF shall not accept the certificate and deny the connection.
- 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.

A Certificate Request is generated as specified in RFC 2986 containing the public key and “Common Name” in order for the TOE to have its own certificate. The chain of certificates is validated from the root CA when the CA Certificate Response is received. In order for the TOE to authenticate to the remote

Syslog and Active Directory servers, trusted CA certificates must be installed into the TOE's certificate trust store.

8.4 Security Management

8.4.1 FMT_MOF.1/ManualUpdate, FMT_MTD.1/CoreData, and FMT_SMF.1

The SFRs listed above have been combined to clarify the Security Management functions of the TOE including how the TOE implements authentication, identification, and also RBAC. The following description will also include restrictions for these roles and functions.

The TOE uses role-based access control (RBAC), as described in FMT_SMR.2, to restrict access to the functions that manage the TSF data. The available functionality that is presented to an authenticated user is based on the group of permissions and the privileges associated with the permissions. These permissions/privileges are bound to the user only after the user has successfully authenticated. Until then the only ability for a user is to see the Warning Banner and present credentials. The Console then limits the presented functionality based on the privileges bound to that user. The TSF restricts the ability to manage the TSF data to only Security Administrators.

The TSF management functions that are restricted to the Security Administrator based on local or remote administration and scoped by this evaluation are:

Management Function	Local CLI (physical connection)	Remote CLI (SSH)	Console (TLS)
Configure Banner Text			X
Configure Idle Session Timeout			X
Initiate Manual Update			X
Configure Failed Lockout Threshold			X
Configure Lockout Duration			X
Configure Cryptographic functionality	X	X	
Re-enable Administrator accounts			X
Configure System Time	X	X	

Table 22: Management Functions to Management Interface Identification

8.4.2 FMT_SMR.2

The TOE is designed to use permissions which allow, limit or prevent user access to specific Console tools (access to the management functions available through the Console). Upon successful authentication, the TSF associates the administratively defined set of permissions for that user to the subject acting on behalf of that user. The TSF then enforces role-based access control (RBAC) to limit access to TSF functions and data based on the set of permissions bound to the subject.

A set of permissions is called a role. The TOE has one pre-defined role: "Admin". The user permissions for the "Admin" role cannot be modified or customized. A user assigned the "Admin" role is the TOE administrator (Security Administrator) and has access to all Console tools and features and is able to administer the TOE locally and remotely. All other users that do not have the full set of administrative permissions are categorized as a "Console User".

Forescout is installed with a user with the "Admin" role with a customized password created during installation by the customer. This means that other users (Console Users) do not need to be created in order to operate the system. However, if other users are desired then this administrative user may create Console Users or additional TOE administrators.

Console Users can be created, deleted or modified by an administrator (or a Console User with the necessary permission). Each Console User must be assigned one or more permissions when created (equivalent of a customizing a role without being able to assign a specialized moniker to the set of permissions selected). A Console User's set of permissions can be customized by adding and subtracting specific permissions to allow/disallow the user TOE functionality or by selecting the "Admin" role to establish another full TOE administrator after creation.

8.5 Protection of the TSF

8.5.1 FPT_APW_EXT.1

No passwords are stored by the TOE in plaintext. All Console user passwords are hashed using SHA-256 and then encrypted using AES-256. CLI user password is hashed using SHA-512. There is no function provided by the TOE to display a password value in plaintext nor is the password data recoverable.

8.5.2 FPT_SKP_EXT.1

The TOE does not provide a mechanism to view pre-shared keys, symmetric keys and private keys. Volatile memory used to store secret keys, private keys, and secret key data is not accessible by administrators and neither is the file system of the OS. Data keys stored on the TOE are encrypted using AES-256. There are no keys stored in plaintext.

8.5.3 FPT_STM_EXT.1

The TOE provides its own time via its internal clock that is set manually. An administrator can set the time using the CLI interface.

The TOE uses the clock for several security-relevant purposes, including:

- Audit records timestamps (seconds, milliseconds, microseconds, or nanoseconds).
- X.509 certificate validation
- Inactivity of remote sessions
- Inactivity of local session

8.5.4 FPT_TST_EXT.1

Upon the startup of the TOE, multiple Power-On Self Tests (POSTs) are run. The POSTs provide environmental monitoring of the TOE's components (hardware and software), in which early warnings can prevent whole component failure.

The following self-tests are performed to verify the integrity of the software and cryptographic modules. The self-tests will also be run on service restarts and will be available for manual execution. The following tests are part of the self-test suite:

#	Component	Validation	Fail Result

1.	Kernel	HMAC + Built-in Crypto Self-test	Hard-fail
2.	Core OS and packages (including OpenSSH)	Built-in RPM Verification	Hard-fail
3.	fipscheck utility	HMAC verified against fipshmac	Hard-fail
4.	Crypto: OpenSSL	fipscheck (including OpenSSL self-check)	Hard-fail
5.	OpenSSL rpm package	Built-in RPM Verification	Hard-fail
6.	Crypto: Bouncy Castle	Built-in crypto package self-test (KAT)	Hard-fail
7.	Core Platform and plugin installation packages and extracted files.	SHA-256 verified against last known or stored hash.	Soft-fail
8.	System current state vs system configuration	Running kernel version compared to version defined in grub; FIPS mode running status compared to configuration in grub.	Soft-fail

Table 23: Self-Test List with Failure Results

Hard-fail: Kernel test failure will result in panic the OS. Machine will not start.

Soft-fail: Upon test failure, the function would alert the Admin on the terminal (upon logon to CLI), write an audit event and send syslog event (if configured). The main TOE service will not start (i.e. not available for operational use), alert will be displayed on the terminal (upon logon to CLI),

These tests are sufficient to validate the correct operation of the TSF because they verify that the software has not been tampered with and that the underlying hardware does not have any anomalies that would cause the software to be executed in an unpredictable or inconsistent manner.

8.5.5 FPT_TUD_EXT.1

The Console provides the Security Administrator a means to query the TOE for the currently executing version of the TOE software.

When an update is available, the Security Administrator may download the update package in the following ways:

- directly to the Console's host platform using the host platform's web browser,
- download to another device and then upload the package to Console's host platform*, or
- by directly using the Console to download the update package

*NOTE: Method used for evaluated configuration testing.

Once the update is on the Console's host platform, an administrator must manually initiate the installation via the Console. There is no automatic update function provided. The Console will upload the update package over the existing TLS path that is already established between the Console and the TOE appliance. The TOE does not automatically download or update itself nor does it connect to the update server directly.

Once the upload is complete, the Console will stimulate the TSF to verify the update's digital signature. The TSF uses a locally stored public key (on the appliance) to verify update package authenticity. This key is installed as part of the initial software installation and cannot be modified or changed by an administrator. The TSF will not continue with the update if the digital signature is determined to be invalid for any reason. There is no means for an administrative override to continue the installation. There is no delay in activiation.as the TOE will reboot upon completion.

8.6 TOE Access

8.6.1 FTA_SSL_EXT.1

When a local session is inactive for the configured period of time the TOE will terminate the session. The inactivity timer can be configured by the Security Administrator using the Console, which is set in minutes.

8.6.2 FTA_SSL.3

The TOE will terminate a remote session due to inactivity according to the configuration threshold set by the Security Administrator. The inactivity timer can be configured by the Security Administrator using the Console to be enabled/disabled and it is set in minutes or hours.

8.6.3 FTA_SSL.4

Any user accessing the TOE is capable of terminating their own Console session by clicking the “Exit” command from the File menu. A user authenticated to the CLI can terminate the current session by typing "quit" at the command line.

8.6.4 FTA_TAB.1

There are three possible administrative ways to log into the TOE: locally via physical connection to access the CLI, remotely via SSH connection to access the CLI, and remotely using the Console which establishes a TLS connection. When logging in locally or remotely, the pre-authentication banner is displayed and is viewed prior to authentication. The authentication banner is administratively customizable.

8.7 Trusted Path/Channels

8.7.1 FTP_ITC.1

The TOE provides the ability to secure sensitive data in transit to and from the Operational Environment. The TOE, acting as the TLS client, uses the TLS protocol to initiate and establish the trusted channel to support the following capabilities:

- to export audit data to a syslog server
- authenticate users via an Active Directory server

The TOE appliance’s TLS client implementation is conformant to FCS_TLSC_EXT.1. TLS communications use X.509v3 certificates to support authentication.

8.7.2 FTP_TRP.1/Admin

Remote administration is secured by using SSH and TLS protocols.

The Console establishes the TLS connection to the TOE appliance on behalf of the user for remote administration. The TOE appliance is acting as a TLS Server and is conformant to FCS_TLSS_EXT.1. The Console is using the host platforms TLS client capabilities.

A user can connect to the TOE appliance using SSH to remotely manage the TOE appliance via the CLI (remote console). The TOE appliance’s SSH server implementation is conformant to FCS_SSHS_EXT.1.