National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Forescout

Report Number: CCEVS-VR-VID11008-2020
Version 1.0
March 16, 2020

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

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

ACKNOWLEDGEMENTS

Validation Team

Tony Chew, The Aerospace Corporation
Marybeth Panock, The Aerospace Corporation
James Donndelinger, The Aerospace Corporation

Common Criteria Testing Laboratory

Herbert Markle
Joshua Jones
Christopher Rakaczky
David Cornwell

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Forescout provided by Forescout Technologies, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in March 2020. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements set forth in the *collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314* (NDcPP).

The Target of Evaluation (TOE) is the Forescout hardware that runs the Forescout software version 8.1. Forescout's primary functionality 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. However, the evaluated TOE functionality includes only the security functional behavior that is defined in the claimed NDcPP.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Evaluation Activities contained in the NDcPP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the NDcPP Evaluation Activities. The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *Forescout Security Target v1.0*, dated January 23, 2020 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Evaluation Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1 – Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Forescout hardware that runs the Forescout software version 8.1. Refer to Table 2 for Model Specifications
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018, including all applicable NIAP Technical Decisions and Policy Letters
Security Target	Forescout Security Target v1.0, dated January 23, 2020
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Forescout" Evaluation Technical Report v1.0 dated January 27, 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Forescout Technologies, Inc.
Developer	Forescout Technologies, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Tony Chew, The Aerospace Corporation Marybeth Panock., The Aerospace Corporation Jim Donndelinger, The Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

- The following assumptions about the operational environment are made regarding its ability to provide security functionality.
- It is assumed that the TOE is deployed in a physically secured operational environment and not subjected to any physical attacks.
- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- The TOE is not responsible for protecting network traffic that is transmitted across its interfaces that is not related to any TOE management functionality or generated data.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that regular software and firmware updates will be applied by a TOE Administrator when made available by the product vendor.
- Administrator credentials are assumed to be secured from unauthorized disclosure.
- It is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack against a TOE component and that auditing is functioning on all TOE components.
- TOE Administrators are trusted to ensure that there is no unauthorized access possible for sensitive residual information on the TOE when it is removed from its operational environment.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.UNAUTHORIZED_ADMINISTRATOR_ACCESS** – Threat agents may attempt to gain Administrator access to the 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.

3.3 Clarification of Scope

- All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP are claimed by the TOE and documented in the ST.

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to security functionality not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. All other functionality provided by these devices, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. The Security Management Platform's capabilities to collect network traffic and events, correlate the data collected to detect threats, and provide recommendations for responses to safeguard the network against cyberattacks described in Section 1.3 of the Security Target were not assessed as part of this evaluation. Further information of excluded functionality can be found in Section 2.3 of the Security Target.

The evaluated configuration of the TOE is the Forescout described in Tables 2,3,4 and 5 running the Forescout software version 8.1. In the evaluated configuration, the TOE uses TLS to secure remote GUI-based administration, SSH to secure remote command-line administration, and TLS to secure transmissions of security-relevant data from the TOE to external entities such as authentication server and syslog. The TOE includes administrative guidance to instruct Administrators in the secure installation and operation of the TOE. Adherence to this guidance is sufficient to ensure that the TOE is operated in accordance with its evaluated configuration.

4 Architectural Information

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

4.1 TOE Introduction

The TOE is the Forescout network device, as defined in the NDcPP which states: “This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a network device… 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… Examples of network devices that are covered by requirements in this cPP include routers, firewalls, VPN gateways, IDSs, and switches”. The TOE consists of the Forescout hardware models that runs the Forescout software version 8.1. Thus, the TOE is a network device composed of hardware and software. The Forescout network device or 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. 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.

4.2 Physical Boundary

The following figure depicts the TOE boundary and operational environment:

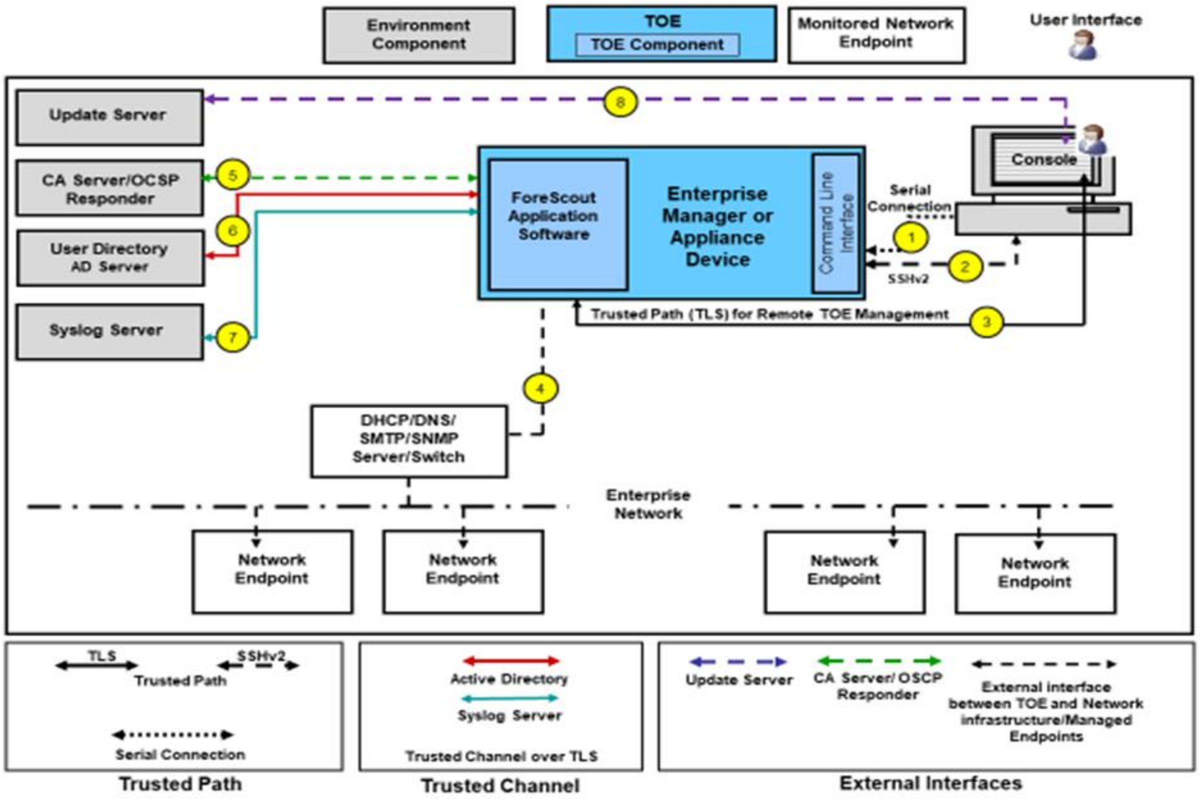


Figure 1: TOE Boundary

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

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 2 – 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	2U Rack-mount

		CEM-150, CEM-200	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 3 - 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 4 - CT/CEM Models Rev50

System Name	Equipment		
Forescout:	**Software/Firmware**	**Hardware**	**Component/Configuration**

Appliance (CT-) **&** **Enterprise Manager (CEM-)**		**Model**	
	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 5 – 51xx Models

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

Component	**Definition**
Certification Authority / OCSP Responder	A server that acts as a trusted issuer of digital certificates and hosts the OCSP Responders that identifies revoked certificates.
Management Workstation	Any general-purpose computer that is used by a Security Administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client to access the CLI or the Forescout Console to access the remote GUI.
Syslog Server	The syslog server connects to the TOE and allows the TOE to send syslog messages to it for remote storage. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.
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. In the evaluated configuration, the TOE connects to a server with Active Directory for its remote authentication store.
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. The TOE does

	not directly communicate with the update server. The TOE receives the update from the Forescout Console.

Table 6 – IT Environment Components

5 Security Policy

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.

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.

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 7: 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, SHA-384	C944
FCS_COP.1/KeyedHash	HMAC-SHA-1, HMAC-SHA-256, HMAC-384	C944
FCS_RBG_EXT.1	Hash DRBG	C944

Table 8: Cryptographic Algorithm Table for Bouncy Castle

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.

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.

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.

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.

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

6 Documentation

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

- Forescout Supplemental Administrative Guidance for Common Criteria version 1.0, December 17, 2019
- Forescout Installation Guide Version 8.1, November 6, 2019
- Forescout Administration Guide Version 8.1, March 20, 2019

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

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Forescout that runs the Forescout software version 8.1. Section 4 describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to directly communicate with the following environment components:

- Management Workstation for local and remote administration
- Active Directory Server for remote authentication
- Syslog Server for recording of syslog data
- Certificate Authority/Online Certificate Status Protocol (OCSP) Responder

To use the product in the evaluated configuration, the product must be configured as specified in the *Forescout Supplemental Administrative Guidance for Common Criteria Version 1.0* document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary *Evaluation Technical Report for a Target of Evaluation "Forescout" Evaluation Technical Report v1.0 dated January 27, 2020*, as summarized in the publicly available *Assurance Activity Report for a Target of Evaluation "Forescout" Assurance Activities Report v1.0 dated January 27, 2020.*

8.1 Test Configuration

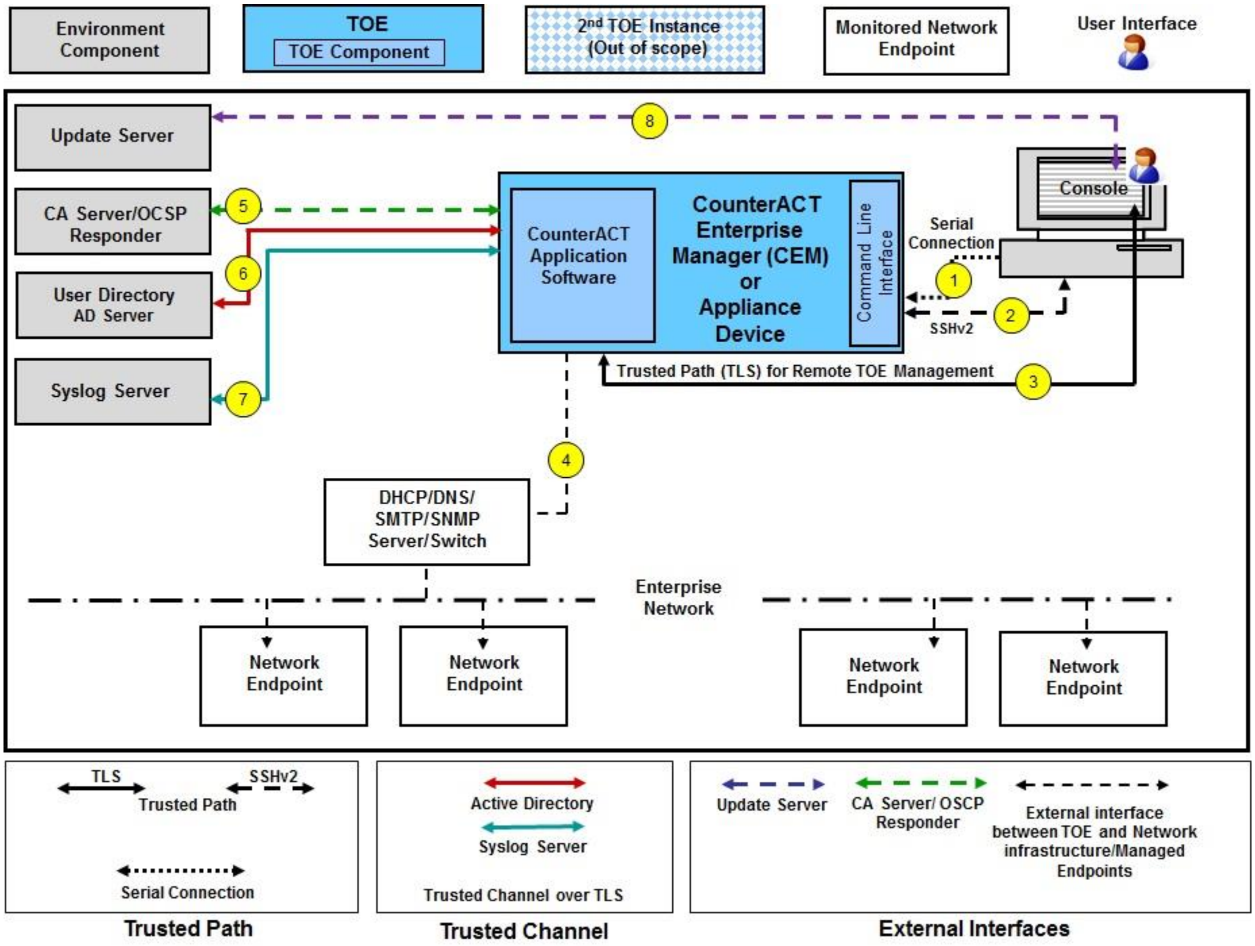
The evaluation team configured the TOE for testing according to the *Forescout Supplemental Administrative Guidance for Common Criteria Version 1.0* (AGD) document. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the Evaluation Activities against the TOE over the SFR relevant interfaces. The evaluation team conducted testing in the Booz Allen CCTL facility on an isolated network. Testing was performed against all three management interfaces defined in the ST (local CLI, remote CLI, and remote GUI).

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

- Management Workstation for local and remote administration
- Syslog Server for recording of syslog data
- Active Directory Server for remote authentication
- Certificate Authority/Online Certificate Status Protocol (OCSP) Responder

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

- Forescout Console Application v8.1
- WireShark: version 2.6.4
- Firefox Quantum: version 68.0.1
- Internet Explorer: version 11.726.16299.0
- Google Chrome: version 75.0.3770.142
- PuTTY SSH Client: version .70
- Tcpdump: version 4.9.2
- Libpcap version 1.8.1
- OpenSSL version 1.0.2k and 1.0.1t
- rsyslogd 8.24.0



Test Configuration

8.2 Developer Testing

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

8.3 Evaluation Team Independent Testing

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

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

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

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

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

The team tested the following areas:

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- Vulnerability Scan (Nessus)
  Nessus is an automated vulnerability scanner and assessment tool. It looks for major vulnerabilities including vulnerable applications and services, as well as less critical vulnerabilities such as unnecessary information disclosure.
- SSH Timing Attack (User Enumeration)
  This attack attempts to enumerate validate usernames for the SSH interface, by observing the difference in server response times to valid username login attempts.
- Force SSHv1
  This attack determines if the SSH server on the TOE will accept an SSHv1 connection when the TOE claims to only support SSHv2

The TOE successfully prevented any attempts of subverting its security.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all Evaluation Activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Forescout product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the NDcPP Supporting Documents in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents related to the examination of the information contained in the TOE Summary Specification.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Evaluation Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Document related to the examination of the information contained in the operational guidance documents.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Evaluation Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work units. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Evaluation Activities in the NDcPP Supporting Documents and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

The validators reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the NDcPP Supporting Documents were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis requirements in the NDcPP Supporting Documents, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Evaluation Activities in the NDcPP Supporting Document, and correctly verified that the product meets the claims in the ST.

10 Validator Comments and Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Forescout Supplemental Administrative Guidance for Common Criteria Version 1.0* document. No versions of the TOE and software, either earlier or later were evaluated.

Administrators should take note of the fact that when the product is configured to offload audit files to an audit logging server, if that communications link is interrupted, the audit files generated during the time of the interruption will be captured locally. However, upon resumption of the connectivity, the offload begins with the reconnection and will NOT send those audit files generated during the outage. It will be necessary for the administrator to take steps to offload those files or they will be overwritten when the audit log is full.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the routers and switches network infrastructure, need to be assessed separately and no further conclusions can be drawn about their effectiveness. Section 2.3 “Excluded from the TOE” of the ST provides the details of features that are part of the purchased product but were not included in the evaluation. These include web portals, Hierarchical Functionality/Trusted Appliance Interface, host scanning, network monitor, network response, HTTP Redirection, SNMP and SMTP support.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Forescout Security Target v1.0,* dated January 23, 2020.

13 List of Acronyms

Acronym	Definition
CA	Certificate Authority
CC	Common Criteria
CLI	Command-Line Interface
cPP	collaborative Protection Profile
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CVL	Component Validation List
DN	Distinguished Name
DNS	Domain Name Server
DRBG	Deterministic Random Bit Generator
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IP	Internet Protocol
IT	Information Technology
KAS	Key Agreement Scheme
KDF	Key Derivation Function
LDAP/AD	Lightweight Directory Access Protocol / Active Directory
NDcPP	Network Device collaborative Protection Profile
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RAM	Random Access Memory
RBG	Random Bit Generator
RU	Rack Unit
SAN	Subject Alternative Name
SAR	Security Assurance Requirement
SCP	Secure Copy Protocol
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface

14 Terminology

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 Forescout, for example desktop, laptop, server, etc.
Enterprise Manager	A Forescout Appliance configured to manage multiple Appliances distributed across the network.
Local console	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 Forescout. Plugins enable deeper inspection as well as broader control over network endpoints. Bundled plugins are pre-packaged with Forescout. 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

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018
6. Forescout Security Target v1.0, dated January 23, 2020
7. Forescout Supplemental Administrative Guidance for Common Criteria Version 1.0, December 17, 2019
8. Forescout Installation Guide Version 8.1, November 6, 2019
9. Forescout Administration Guide Version 8.1, March 20, 2019
10. Assurance Activities Report for a Target of Evaluation Forescout Security Target, Version 1.0, January 27, 2020
11. Evaluation Technical Report for a Target of Evaluation Forescout, Version 1.0, January 27, 2020