Forescout v8.3
Supplemental Administrative Guidance for Common Criteria

Version 1.0

June 1, 2022

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 Street
Laurel, MD 20707

Contents

Table of Tables

1 Introduction

Forescout is a hardware appliance whose primary functionality is related to the handling of network traffic. The Collaborative Protection Profile for Network Devices, version 2.2e (NDcPP) defines a network device as "a device that is connected to a network and has an infrastructure role within that network. The TOE may be standalone or distributed, where a distributed TOE is one that requires multiple distinct components to operate as a logical whole in order to fulfil the requirements of this cPP…" Additionally, the NDcPP says that example devices that fit this definition include "physical and virtualised routers, firewalls, VPN gateways, IDSs, and switches."

As a Common Criteria evaluated product, this guidance serves to define the 'evaluated configuration' in which the evaluation was performed and to summarize how to perform the security functions that were tested as part of the evaluation.

2 Intended Audience

This document is intended for administrators responsible for installing, configuring, and/or operating Forescout. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation. The reader is expected to be familiar with the general operation of the Forescout product. This supplemental guidance includes references to Forescout's standard documentation set for the product and does not explicitly reproduce materials located there.

The reader is also expected to be familiar with the Forescout Security Target and the general CC terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions for how to perform the security functions that are defined by these SFRs. The Forescout product as a whole provides a great deal of security functionality but only those functions that were in the scope of the claimed PP are discussed here. Any functionality that is not described here or in the Forescout Security Target was not evaluated and should be exercised at the user's risk.

3 Terminology

In reviewing this document, the reader should be aware of the terms listed below.

CC: stands for Common Criteria. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

SFR: stands for Security Functional Requirement. An SFR is a security capability that was tested as part of the CC process.

TOE: stands for Target of Evaluation. This refers to the aspects of the Forescout product that contain the security functions that were tested as part of the CC evaluation process.

4 References

The following security-relevant documents are included with the TOE. This is part of the standard documentation set that is provided with the product. Documentation that is not related to the functionality tested as part of the CC evaluation is not listed here.

[1] Forescout Installation Guide Version 8.3
[2] Forescout Administration Guide Version 8.3

The following document was created in support of the Forescout CC evaluation:

[3] Forescout v8.3 Security Target Version 1.3 (ST)

4.1 Accessing additional Documentation

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

To access the Documentation Portal:

Accessible for everyone:

https://www.forescout.com/company/resources/

For PAL customers:

https://updates.forescout.com/support/files/counteract/docs_portal/

For Flexx customers:

https://forescout.force.com/support/s/downloads

5 Evaluated Configuration of the TOE

This section lists the components that have been included in the TOE's evaluated configuration, whether they are part of the TOE itself or environmental components that support the security behavior of the TOE:

5.1 TOE Components

The TOE is Forescout, running the Forescout software version 8.3. Forescout is a rack-mounted hardware device. The evaluated models' specific hardware and configuration is as follows:

System Name	Equipment		
	Software/Firmware	**Hardware Model**	**Component/Configuration**
Forescout: Appliance (CT-) & Enterprise Manager (CEM-)	Forescout v8.3 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 1: CT-R Model Rev22

System Name	Equipment		
	Software/Firmware	**Hardware Model**	**Component/Configuration**
Forescout: Appliance (CT-) & Enterprise Manager (CEM-)	Forescout v8.3 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 2: CT/CEM Models Rev40

System Name	Equipment		
	Software/Firmware	**Hardware Model**	**Component/Configuration**
Forescout: Appliance (CT-) & Enterprise Manager (CEM-)	Forescout v8.3 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)
			1x 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)

System Name		Equipment	
			1 USB 2.0 and 1 micro-USB 2.0 (front), 2 USB 3.0 (Rear)
			1x 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 3: CT/CEM Models Rev50

System Name	Equipment		
	Software/Firmware	**Hardware Model**	**Component/Configuration**
Forescout: Appliance (CT-) & Enterprise Manager (CEM-)	Forescout v8.3 operating on CentOS 7.5	4130	1U Rack-mount
			1 HDD
			4 x USB 3.1 Gen2 2 x USB 3.1 Gen1
			Gen 8 Intel® Core™ i5-8500T (Coffee Lake)
			6 x Intel-based NIC Ethernet Ports
		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 4114 (Skylake)

System Name		Equipment	
			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 4: 4130 and 51xx Models

5.2 Supporting Environmental Components

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

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 2GB memory
	  o 1GB disk space
	• OS running:
	  o Windows 7/8/8.1/10
	  o Windows Server 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019
	  o Linux RHEL/CentOS 7 / 8
	  o macOS 10.12 / 10.13 / 10.14 / 10.15 / 11
	  o 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.
	
	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).

Active Directory Server	A system that is capable of receiving authentication requests over TLS and validating these requests against identity and credential data that is defined in the directory (Microsoft version of an LDAP Server). The TOE is the TLS client for this communication.
Audit Server	The TOE connects to an audit server to send the audit records 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.
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.
Network Infrastructure	The network infrastructure contains components such as routers, switches, DNS server, etc. Figure 1 identifies these interfaces as a single interface. The interface to the managed network infrastructure is a separate connection to the enterprise operational environment the TOE is managing. The TOEs management of the enterprise operational environment is out of scope for the NDcPP. Therefore, this interface is out of scope of the evaluation.
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. This interface is out of scope of the evaluation. It is being declared as part of the test environment for completeness as it is used to support trusted updates testing.

Table 5: Supporting Components in the Operational Environment

5.3 Assumptions

In order to ensure the product is capable of meeting its security requirements when deployed in its evaluated configuration, the following conditions must be satisfied by the organization, as defined in the claimed Protection Profile:

- **Physical security:** The Forescout product does not claim any sort of physical tamper-evident or tamper-resistant security mechanisms. Therefore, it is necessary to deploy the product in a locked or otherwise physically secured environment so that it is not subject to untrusted physical modification.
- **Limited functionality:** The Forescout product must only be used for its intended networking purpose. General purpose computing applications, especially those with network-visible interfaces, may compromise the security of the product if introduced.
- **No through traffic protection:** The security boundary of the Common Criteria evaluation is limited to traffic flowing to or from the TOE. The intent is for Forescout 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 NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
- **Trusted administration:** The Forescout product does not provide a mechanism to protect against the threat of a rogue or otherwise malicious administrator. Therefore, it is the responsibility of the organization to perform appropriate vetting and training for security administrators prior to granting them the ability to manage the product. The security administrators will also fully validate any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store as a trust anchor prior to use.
- **Regular updates:** Forescout provides regular product updates for the Forescout product that include bug fixes as well as functionality and security enhancements. It is expected that

administrators are reasonably diligent in ensuring that software patches are applied regularly as they are made available.

- **Secure admin credentials:** Forescout protects the administrator's credentials stored on Forescout that are used to access it. Additionally, it is assumed that any administrative credentials maintained by an environmental AD Server are secured in order to mitigate the risk of impersonation.
- **Residual information:** It is the responsibility of the administrator to 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.

6 Secure Acceptance, Installation, and Configuration

Documentation for how to order and acquire the TOE is described under the Contact Us link on the Forescout website https://www.forescout.com/. Section 5.1 of this document lists the models that are associated with the TOE. When receiving delivery of the TOE, this documentation should be checked as part of the acceptance procedures so that the correctness of the hardware can be verified.

Physical installation and first-time setup of the TOE can be accomplished by following the instructions outlined in [1]. The following must be considered when following these procedures:

1. In the 'Security and Compliance and RMM' section, the steps under the 'FIPS Compliance' section must be performed.
2. In the 'Network Setup' section, the steps under the 'Creating an Out-of-Band IP Management Interface' section are to be performed.
3. Depending on if the Forescout device is being configured as an Appliance or Forescout Enterprise Manager (CEM), only the procedures in the 'Appliance Setup and Configuration and Post-Installation' section or the 'EM Setup and Configuration and Post-Installation' section need to be completed with the exception of the following procedures:
    a. Configure password protection for the boot loader by following the steps under 'Configure Password Protection for the Boot Loader' section of the 'Appliance Setup and Configuration and Post-Installation' section for both an Appliance and CEM.
    b. Disable ICMP by following the steps under the 'Configure ICMP Settings' section of the 'Appliance Setup and Configuration and Post-Installation' section for both an Appliance and CEM.
    c. The use of iDRAC functionality was not assessed in the evaluation. Procedures for enabling this functionality in the 'Appliance Setup and Configuration and Post-Installation' section or the 'EM Setup and Configuration and Post-Installation' section in [1] are not to be performed to configure the devices into their evaluated configuration.

6.1 Enable FIPS Mode

In order to get the TOE into its evaluated configuration, FIPS Mode must be enabled to utilize the evaluated cryptographic algorithms. This step is only needed if FIPS was not enabled during installation.

1. Once all of the plugins are installed and updated, authenticate to the CLI.

2. Enter the command “fstool fips”
3. Follow the prompt to enable/disable FIPS mode.

NOTE: Once the TOE is placed in FIPS mode it only uses the cryptography implementations and algorithms described in the ST for all claimed cryptographic operations:

SFR	OpenSSL Implementation CAVP #C1887 and #A1941	Bouncy Castle Implementation CAVP #C1888 and #A1959
FCS_CKM.1	RSA per FIPS 186-4 Key Generation	N/A
	FFC using Diffie-Hellman group 14, per RFC 3526 Section 3	N/A
FCS_CKM.2	RSA Key Establishment per RSAES-PKCS-v1_5	RSA Key Establishment per RSAES-PKCS-v1_5
	Diffie-Hellman group 14 Key Establishment RFC 3526 Section 3	N/A
FCS_COP.1/ DataEncryption	AES CTR: 128 and 256 bits AES CBC: 128 and 256 bits AES GCM: 128 and 256 bits	AES CBC: 128 and 256 bits AES GCM: 256 bits
FCS_COP.1/SigGen	RSA FIPS 186-4 Signature Services 2048 bits	RSA FIPS 186-4 Signature Services 2048 bits
FCS_COP.1/ Hash	SHS: SHA-1, SHA-256, SHA-384, and SHA-512	SHS: SHA-1, SHA-256, and SHA-384
FCS_COP.1/KeyedHash	HMAC-SHA-1, HMAC-SHA-256, HMAC-384, and HMAC-SHA-512	HMAC-SHA-1, HMAC-SHA-256, and HMAC-384
FCS_RBG_EXT.1	CTR DRBG	Hash DRBG

Table 6: Cryptographic Algorithms Implemented in FIPS enabled mode

For more information regarding FIPS Mode, see the ‘FIPS Compliance’ section in the ‘Appliance Setup and Configuration and Post-Installation’ section in [1].

6.2 Install the Console to Management Workstation

Once initial installation of the TOE has been completed, the Console must be installed on the Management Workstation (refer to Section 5.2 of this document for requirements) to continue configuration of the device into its evaluated configuration as well as to manage the TOE in its operational state.

1. In the web browser type http://<ip address configured for TOE>/install. Note: This is also described on the last screen of the configuration.

2. For a Management Workstation running a Windows OS, select Windows option and the Console download automatically starts.
3. Run the .exe file that was downloaded to install the Console.
4. Once the Console is installed, open the Console and login with the password that was created during the configuration.

For more information on the installation of the Console, see the 'Install and Log in to the Forescout Console' section of [1].

Any of the methods of installation are acceptable. Once installed, open the Console and login with the username and password that was created during the configuration of the Forescout device being connected to. Once authenticated, continue the procedures in the 'Install and Log in to the Forescout Console' section of [1].

Once the TOE is installed and placed into FIPS mode, the TOE acts as a TLS server for the Console connection and will only accept v1.2 requests with the following ciphers:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

This is automatically configured on both the TOE and the Console application. No additional configuration is necessary. The TOE does not claim support session resumption or session tickets.

6.3 Upgrading the TOE

Once configuration through the initial setup wizard is complete, it is recommended that a Security Administrator acquire the latest software image for the current version from Forescout and perform a software upgrade to the current version. To install the new software image, perform the following steps:

1. Place the software image, previously downloaded from Forescout's support portal, on the Management Workstation.
2. Authenticate to the TOE via the Console using a Security Administrator account.
3. Check the current version of the TOE software and plugins:
    a. Navigate to "Help" > "About Forescout".
    b. Navigate to "Tools" > "Options" > "Modules".
    c. Notate the version and build number.
4. Install the latest software image:
    a. Navigate to "Tools" > "Options" > and:
        i. If on an Enterprise Manager, select "CounterACT Devices".
        ii. If on an Appliance, select "Appliance".
    b. Click "Upload and Upgrade".
    c. Specify the update file (e.g., service pack) and click "Install".
    d. Once the update file has been fully uploaded, the TOE will verify the digital signature of the update file and:
        i. If the digital signature verification check is successful, the update process will continue and the next procedure to be followed is Step 5.

ii. If the digital signature verification check is unsuccessful, the update process is halted:
    1. A warning banner will appear notifying the administrator of the failed attempt.
    2. The next procedure to be followed is Step 8.

5. Proceed through the dialog boxes of the wizard to install the update.
6. After an update finishes installing, the TOE will normally reboot.
7. If individual plugin files have been provided for update as well:
    a. Navigate to "Tools" > "Options" > "Modules" > "Install".
    b. Specify the plugin update file.
8. Once the update file has been fully uploaded, the TOE will verify the digital signature of the update file and:

    Repeat Step 3 and:
    a. If the installation was successful, verify that the currently installed version corresponds to that of the update.
    b. If the installation was unsuccessful, verify that the currently installed version remains unchanged from the original execution of Step 3.

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. For more information on upgrading the TOE, see the 'Managing Appliances, Enterprise Managers, and Consoles' section in [2].

6.4 Power-On Self Tests

Upon the startup of the TOE in the evaluated configuration, 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 TOE must be configured to run the POSTs by following these procedures:

1. Authenticate to the TOE via the CLI using a Security Administrator account.
2. Execute the following command:

```
fstool get_property fs.selftest.enable
```

3. If the command in Step 2 returns `"fs.selftest.enable="` then execute the following command to enable self-tests:

```
fstool set_property fs.selftest.enable true
```

The following self-tests are performed to verify the integrity of the software and cryptographic modules. The self-tests are also run on service restarts and are 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 CounterACT 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 7: 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 local CLI Security Administrator upon login, write an audit event and send the audit record to the external audit server (if configured). The main Forescout service will not start (e.g., not available for operational use), alert will be displayed on the the local 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.

In the event that a POST fails, the TOE will need to be rebooted. If the TOE has been corrupted or the hardware has failed such that rebooting will not resolve the issue, a Security Administrator will need to contact Forescout support per the guidance in Section 10 of this document.

A CLI Security Administrator may run the self-test check manually from the CLI.

1. Authenticate to the TOE via the CLI using a Security Administrator account.
2. Execute the following command:

```
selftest
```

3. Enter password for user.

An example of a successful execution of the command:

```
selftest:144141:1628543527.855930:Mon Aug  9 17:12:07 EDT -0400 2021: Started
selftest:144141:1628543527.856168:Mon Aug  9 17:12:07 2021: Verifying fipscheck
selftest:144141:1628543527.912380:Mon Aug  9 17:12:07 2021: Verifying grub
selftest:144141:1628543527.936682:Mon Aug  9 17:12:07 2021: Verifing rpm: kernel (64-bit)
selftest:144141:1628543528.053546:Mon Aug  9 17:12:08 2021: Verifing rpm: glibc (64-bit)
selftest:144141:1628543528.104342:Mon Aug  9 17:12:08 2021: Verifing rpm: glibc
selftest:144141:1628543528.738303:Mon Aug  9 17:12:08 2021: Verifing rpm: openssl (64-bit)
selftest:144141:1628543528.806710:Mon Aug  9 17:12:08 2021: Verifing rpm: openssl
selftest:144141:1628543529.006420:Mon Aug  9 17:12:09 2021: Verifing rpm: openssh
selftest:144141:1628543529.218141:Mon Aug  9 17:12:09 2021: Verifing rpm: openssh-server
selftest:144141:1628543529.383394:Mon Aug  9 17:12:09 2021: Verifing rpm: openssh-clients
selftest:144141:1628543529.596567:Mon Aug  9 17:12:09 2021: Verifying plugin: ad
selftest:144141:1628543532.249591:Mon Aug  9 17:12:12 2021: Verifying plugin: appframework
selftest:144141:1628543533.395501:Mon Aug  9 17:12:13 2021: Verifying plugin: atc
selftest:144141:1628543533.998487:Mon Aug  9 17:12:13 2021: Verifying plugin: aws
```

selftest:144141:1628543538.699878:Mon Aug 9 17:12:18 2021: Verifying plugin: azure
selftest:144141:1628543540.003110:Mon Aug 9 17:12:20 2021: Verifying plugin: cef
selftest:144141:1628543540.463807:Mon Aug 9 17:12:20 2021: Verifying plugin: classification
selftest:144141:1628543540.962202:Mon Aug 9 17:12:20 2021: Verifying plugin: cloud_configuration
selftest:144141:1628543541.854176:Mon Aug 9 17:12:21 2021: Verifying plugin: cloud_net
selftest:144141:1628543543.009764:Mon Aug 9 17:12:23 2021: Verifying plugin: datapublisher
selftest:144141:1628543543.879623:Mon Aug 9 17:12:23 2021: Verifying plugin: datareceiver
selftest:144141:1628543545.146556:Mon Aug 9 17:12:25 2021: Verifying plugin: devicedatacollector
selftest:144141:1628543545.765749:Mon Aug 9 17:12:25 2021: Verifying plugin: dhclass
selftest:144141:1628543546.031744:Mon Aug 9 17:12:26 2021: Verifying plugin: dns_client
selftest:144141:1628543546.239343:Mon Aug 9 17:12:26 2021: Verifying plugin: dnsniff
selftest:144141:1628543546.471452:Mon Aug 9 17:12:26 2021: Verifying plugin: dot1x
selftest:144141:1628543549.175320:Mon Aug 9 17:12:29 2021: Verifying plugin: epm
selftest:144141:1628543549.602948:Mon Aug 9 17:12:29 2021: Verifying plugin: extcls
selftest:144141:1628543549.822939:Mon Aug 9 17:12:29 2021: Verifying plugin: flow
selftest:144141:1628543550.340467:Mon Aug 9 17:12:30 2021: Verifying plugin: goodies
selftest:144141:1628543550.589499:Mon Aug 9 17:12:30 2021: Verifying plugin: hijack_assist
selftest:144141:1628543550.799895:Mon Aug 9 17:12:30 2021: Verifying plugin: hwi
selftest:144141:1628543551.058744:Mon Aug 9 17:12:31 2021: Verifying plugin: linux
selftest:144141:1628543553.316870:Mon Aug 9 17:12:33 2021: Verifying plugin: meta
selftest:144141:1628543553.610693:Mon Aug 9 17:12:33 2021: Verifying plugin: ms
selftest:144141:1628543564.930685:Mon Aug 9 17:12:44 2021: Verifying plugin: nbtscan_plugin
selftest:144141:1628543565.192814:Mon Aug 9 17:12:45 2021: Verifying plugin: nc
selftest:144141:1628543566.061682:Mon Aug 9 17:12:46 2021: Verifying plugin: ncc
selftest:144141:1628543566.322827:Mon Aug 9 17:12:46 2021: Verifying plugin: netflowtool
selftest:144141:1628543566.586827:Mon Aug 9 17:12:46 2021: Verifying plugin: nic
selftest:144141:1628543566.862243:Mon Aug 9 17:12:46 2021: Verifying plugin: nsx
selftest:144141:1628543567.569983:Mon Aug 9 17:12:47 2021: Verifying plugin: osx
selftest:144141:1628543568.362324:Mon Aug 9 17:12:48 2021: Verifying plugin: otsm
selftest:144141:1628543570.008946:Mon Aug 9 17:12:50 2021: Verifying plugin: pe
selftest:144141:1628543570.236059:Mon Aug 9 17:12:50 2021: Verifying plugin: posture
selftest:144141:1628543571.021710:Mon Aug 9 17:12:51 2021: Verifying plugin: posturelib
selftest:144141:1628543571.313295:Mon Aug 9 17:12:51 2021: Verifying plugin: profiles
selftest:144141:1628543571.962343:Mon Aug 9 17:12:51 2021: Verifying plugin: rogued
selftest:144141:1628543572.270699:Mon Aug 9 17:12:52 2021: Verifying plugin: scc
selftest:144141:1628543572.823495:Mon Aug 9 17:12:52 2021: Verifying plugin: sms
selftest:144141:1628543573.453797:Mon Aug 9 17:12:53 2021: Verifying plugin: spt
selftest:144141:1628543574.824271:Mon Aug 9 17:12:54 2021: Verifying plugin: support
selftest:144141:1628543575.572365:Mon Aug 9 17:12:55 2021: Verifying plugin: sw
selftest:144141:1628543579.434284:Mon Aug 9 17:12:59 2021: Verifying plugin: syslog
selftest:144141:1628543579.694383:Mon Aug 9 17:12:59 2021: Verifying plugin: va
selftest:144141:1628543581.241262:Mon Aug 9 17:13:01 2021: Verifying plugin: vmware
selftest:144141:1628543581.795053:Mon Aug 9 17:13:01 2021: Verifying plugin: vpn3k
selftest:144141:1628543582.425514:Mon Aug 9 17:13:02 2021: Verifying plugin: webgui

selftest:144141:1628543584.459167:Mon Aug 9 17:13:04 2021: Verifying plugin: webreports
selftest:144141:1628543586.961391:Mon Aug 9 17:13:06 2021: Verifying plugin: wireless
selftest:144141:1628543587.926005:Mon Aug 9 17:13:07 2021: Verifying Bouncy Castle
selftest:144141:1628543589.825786:Mon Aug 9 17:13:09 2021: Verifying hf files
selftest:144141:1628543589.840081:Mon Aug 9 17:13:09 2021: Done

An example of an error found:

selftest:16201:1628544440.566558:Mon Aug 9 17:27:20 2021: problem plugin: hwi, plugin/hwi/scripts/hwi_cert_store_new.exe, file sha256sum, 6e23399aabb23038e07151c67b2c9008753509ee2d675b4a0d81d63744590c04 != c6f0d923ce293167507206795b3f3b982e6c8057a1929231f9ff86eb4753e9bf

6.5 Set up SSH

The TOE acts as an SSH server for remote CLI management. The TOE is configured to support the following algorithms for SSH in the evaluated configuration:

- Encryption algorithms: aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com
- Public key algorithms: ssh-rsa
- MAC algorithms: hmac-sha1, hmac-sha2-256, hmac-sha2-512
- Key exchange method: diffie-hellman-group14-sha1

NOTE: The MAC algorithms defined above are the only ones included in the evaluated configuration and thus, the “none” MAC algorithm is never allowed for SSH. Also, when the encryption algorithm uses GCM, GCM is implicitly used as the MAC algorithm.

SSH public key authentication can be achieved for SSH by a CLI Security Administrator executing the following steps for a user’s account:

1. On the SSH client, generate a new public/private key pair.
2. Export the public key using OpenSSH format.
3. Authenticate to the TOE CLI with username and password.
4. Type “user auth setkey”.
5. Select the user to add authentication for.
6. Paste in the public key and press enter.

SSH session key thresholds for time and amount of transmitted data can be configured by a CLI Security Administrator executing the following steps:

1. Authenticate to the TOE via the CLI using a Security Administrator account.
2. Execute the following command:

```
ssh -t server -o RekeyLimit "1G 1h"
```

The settings shown in this command are both the maximum and default values for the evaluated configuration. In this configuration, the TOE has been configured to rekey when one hour has elapsed or

one gigabyte of data has been transmitted using a key; whichever occurs first. The first argument in the quotation marks specifies the maximum amount of data that may be transmitted before the session key is renegotiated. This value is defined in bytes and may have a suffix of 'K', 'M', or 'G' to indicate Kilobytes, Megabytes, or Gigabytes, respectively. The second argument in the quotation marks specifies the maximum amount of time that may pass before the session key is renegotiated. This value is defined with a suffix of 's', 'm', or 'h' to indicate seconds, minutes, or hour respectively.

6.6 Certificate Management

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.

Generating Certificate Signing Requests

In order for the TOE to have its own certificate, a certificate signing request must be generated on the TOE and signed by a CA.

Generate a certificate signing request by completing the following procedures:

1. Authenticate to the TOE via the Console using a Security Administrator account.
2. Navigate to "Tools" > "Options" > "Certificates" > "System Certificates"
3. On the right of the screen click "Generate CSR"
4. Complete the following fields (bolded fields are necessary for the Common Criteria evaluation and underlined fields have the required selection made):
    a. **Scope – All\All**
    b. **Common Name – <fully qualified domain name (FQDN) only>**
    c. Organization – <organizational name>
    d. Organizational Unit – <unit name>
    e. Locality – <locality name>
    f. State – <state name>
    g. Country Code – <country code>
    h. Email Address - <email address>
    i. **Key Length – RSA-2048**
    j. **Signature Algorithm – SHA-256**
    k. Validity – <years>
5. Click "Next"
6. When the CSR is generated, scroll down to ensure the public key and common name are present.

For more information on generating a certificate signing request refer to [2]. The procedures above are the ones used during the evaluation which correspond to the 'Generate a CSR for a New System Certificate' section of Appendix H: Configuring the Certificate Interface in [2].

Importing Trusted CA Certificates

In order for the TOE to authenticate to the remote audit and Active Directory servers, trusted CA certificates must be installed into the TOE's certificate trust store. The Common Name and Subject Alternative Name (FQDN only) are the only reference identifiers in the certificate that are 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, service name reference identifiers, or pinned certificates.

Import the required trusted CA certificates by completing the following procedures:

1. Authenticate to the TOE via the Console using a Security Administrator account.
2. Navigate to “Tools” > “Options” > “Certificates” > “Trusted Certificates”.
3. Click “Add”.
4. Specify the Certificate file.
5. Ensure “Enable trusting this certificate” is checked.
6. Click “Next”.
7. Click “Next” after reviewing the certificate data.
8. If on an Appliance:
    a. Ensure “All subsystems” is selected and then click “Finish”.
9. If on an Enterprise Manager:
    a. Ensure “All subsystems” is selected and then click “Next”.
    b. Ensure “All CounterACT devices” is selected and then click “Finish”.
10. Click “Apply”.

For more information on importing trusted CA certificates refer to [2]. The procedures above are the ones used during the evaluation which correspond to the ‘Import and Configure Trusted Certificates’ section of Appendix H: Configuring the Certificate Interface in [2].

Certificate Validation Requirements:

The TOE uses X.509v3 certificates to support authentication for TLS connections to external IT entities in accordance with RFC 5280. The TOE performs certificate validity checking for all outbound TLS connections as part of the connection process. Successful certificate validation is required in order to successfully negotiate a connection.

When the TSF cannot determine the validity of a certificate, the TSF will not accept the certificate and not establish a 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 treats 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 validates 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 validates the certificate revocation status using the Online Certificate Status Protocol (OCSP) as specified in RFC 6960. This includes the leaf certificate and all intermediate certificates received.
- When the TSF cannot establish a connection to determine the validity of a certificate the TSF does not accept the certificate and denies the connection.
- The TSF validates the extendedKeyUsage field according to the following rules:

- Certificates used for trusted updates and executable code integrity verification must 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 must 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 must 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 must have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

The TOE does not validate the entries of any other fields or extensions not described above and would therefore be considered trivially satisfied as part of the X.509 certificate validation.

6.7 Set up connection to an Audit Server

The TOE performs auditing of all audit events required by Common Criteria and stores them locally in the TOE database. This includes audit records for Console and CLI management actions, and individual plugins (e.g., AD client). The TOE provides an interface for remote transmission of these audit records. In the evaluated configuration, this interface is secured using v1.2 and the following ciphersuites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

The audit server will need to support TLS protocol version 1.2 and one of these ciphersuites for communication between the TOE and audit server to be established.

Perform the following procedures to configure the syslog plugin such that the TOE can securely transmit audit data to the audit server:

1. Authenticate to the TOE via the Console using a Security Administrator account
2. Navigate to “Tools” > “Options” > “Modules” > “Core Extensions” > “Syslog”.
3. Select “Configure”.
4. Select “Add” and enter the relevant information for the following fields:
    a. Specify the remote audit server hostname or IP address
    b. Specify the remote audit server port
    c. Specify the server protocol as TCP
    d. Ensure “Use TLS” is checked
    e. Specify an identity for the transmitted audit events
    f. Specify the Facility: local4
    g. Specify the Priority: debug
5. Navigate to the “Default Action Configuration” tab.
6. Specify the following fields:
    a. Specify the remote audit server hostname or IP address
    b. Specify the remote audit server port 6514
    c. Specify the server protocol as TCP
    d. Specify an identity for the transmitted audit events

e. Specify the Facility: local4
f. Specify the Priority: debug

7. Select OK.
8. On the Syslog Triggers tab, ensure "Include operating system messages" is checked.

Once a connection to the audit server is configured, all audit records are stored locally and automatically transferred to the remote audit server as soon as they are generated.

Since syslog functions in a streaming fashion, a communications outage between the TOE and audit server will result in audit data only being recorded locally on the TOE. No special action needs to be taken in the event of a communications outage; no data will be transmitted without encryption and transmissions will automatically resume once communications have been re-established.

6.8 Set up Active Directory Server

An Active Directory Server may be used as a method for user authentication to the Console instead of locally-defined usernames and passwords. In the evaluated configuration, this interface is secured using TLS v1.2 and the following ciphersuites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

The Active Directory Server will need to support TLS protocol version 1.2 and one of these ciphersuites for communication between the TOE and Active Directory Server to be established.

Perform the following procedures to configure the use of an Active Directory Server by the TOE:

1. Authenticate to the TOE via the Console using a Security Administrator account.
2. Navigate to "Tools" > "Options" > "User Directory".
3. Click "Add".
4. Specify the Name field with a description such as "AD".
5. Specify the Type as "Microsoft Active Directory".
6. Ensure "Use as directory", "Use for authentication", and "Use for CounterACT Login" are checked.
7. Click "Next".
8. Specify the Fully Qualified Domain Name of the Active Directory server in the "Address" field.
9. Specify the TLS port for secure LDAP (e.g., 636) and ensure "Use TLS" is checked.
10. Specify the domain, administrator bind account, and password data.
11. Click "Next".
12. Specify the test user data in order to verify that the Active Directory configuration was setup correctly.
13. Click "Finish".
14. Select the newly created User Directory and click "Edit".
15. On the "Advanced" tab, check "Verify user directory server certificate", "Check user directory certificate revocation status using:", and "OCSP".
16. Click "OK".
17. Click "Apply".

18. Click “Test” to verify that the configuration was setup correctly.
19. From the Forescout Options panel, select “Console User Profiles”.
20. Click “Add”.
21. Specify “Single – External User Directory” for the User Type.
22. Specify the external AD username in the User Name field.
23. Select the Server Name that was chosen in Step 4 (e.g., AD).
24. Click “Next”.
25. Specify the permissions for that user on the Forescout device.
26. Click “Next”.
27. Click “Finish”.

For more information on Active Directory Server refer to [2]. The procedures above are the ones used during the evaluation which correspond to the ‘Initial Setup Wizard – User Directory’ section and the ‘User Directory Settings’ section of Appendix I: Security Deployment Hardening Best Practices in [2].

If the Active Directory Server cannot be reached due to a communication outage, it cannot be used to perform authentication. No special action needs to be taken in the event of a communications outage; no data will be transmitted without encryption and once the communication outage is fixed the next authentication request using Active Directory stored username and password will operate as normal. To ensure availability, users can still authenticate using locally defined usernames and passwords.

6.9 Cryptographic Configuration Notice

The administrator installing the TOE is expected to perform all of the operations in Section 6 of this document. This will result in the TOE’s cryptographic operations being limited to the claims made within the Common Criteria evaluation. There is no further configuration required on the TOE’s cryptographic engine as the TOE already becomes pre-configured to meet many of the Common Criteria requirements and the procedures in Section 6 have the administrator manually configuring the remaining items. For this reason, other configurations require no further administrative action.

NOTE: The use of other cryptographic engines and cryptographic settings were not evaluated nor tested during the Common Criteria evaluation of the TOE.

NOTE: There are no known instances where key destruction does not happen as defined by a Security Target [3].

6.10 Security Administrator Accounts

The TOE has one predefined Console administrative user called “Admin”. The “Admin” account is assigned the “administrator” role and these permissions cannot be modified or customized. A customized password must be created during installation by the customer. The “Admin” account is used to create additional Console Security Administrators.

Additionally, the TOE has one predefined CLI administrative role called “cliadmin”. CLI roles and permissions cannot be modified or customized at any time. A CLI Security Administrator is able to administer the TOE locally and remotely via SSH. A customized password must be created during installation by the customer. The “cliadmin” account is used to create additional CLI Security Administrators.

Multiple Console and CLI Security Administrator accounts are required to prevent complete user lockout. During installation and configuration of the TOE, the "Admin" user must create at least one new Console Security Administrator account and the "cliadmin" user must be used to create at least one new CLI Security Administrator account. These new Security Administrator accounts will provide the ability to unlock accounts that have been locked due to reaching the failed number of authentication attempts threshold. See Section 7.3 of this document for instructions on creating new Console and CLI user accounts.

7 Secure Management of the TOE

The following sections provide information on managing TOE functionality that is relevant to the claimed Protection Profile. Note that this information is largely derived from [2] but summarized here to discuss only actions that are required as part of the 'evaluated configuration'. The Security Administrator is encouraged to reference this document in full in order to have in-depth awareness of the security functionality of the Forescout product, including functions that may be beyond the scope of this evaluation.

7.1 Authenticating to the TOE

Users must authenticate to the TOE in order to perform any management functions. Users can authenticate to the TOE locally or remotely. Local users can gain access to the TOE by connecting directly to the TOE which accesses the local console (local CLI) and requires authenticating with their native username/password combination. Remote users can gain access to the TOE by either the remote console (remote CLI) or the Console application. The remote CLI is protected by SSH and allows users to authenticate with either their native username/password combination or SSH public key. To connect to the TOE with SSH requires the SSH client to support specific encryption algorithms, a public key algorithm, MAC algorithms, and a key exchange method, which is describe in Section 6.5 of this document. Section 6.5 also provides the steps to configure the public key authentication for SSH.

The Console application to TOE connection is protected by TLS and allows users to authenticate with either their native username/password combination or their username/password combination stored in an Active Directory server. Section 6.8 of this document describes configuring the TOE to connect to the Active Directory Server. In the evaluated configuration, this management interface is secured using TLS v1.2 and the following ciphersuites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

7.1.1 Log in to Console

1. Launch the Forescout Console application from the Management Workstation.
2. Enter the CounterACT device IP address or host name in the IP/Name filed.
3. Select a login method "Password" to perform authentication.
4. Enter the username and password.

5. Select “Log In.”

For more information regarding accessing the TOE via the Console Application refer the ‘Log In to the Forescout Console’ section of the ‘Welcome to Forescout’ section in [2].

7.1.2 Log in to Local CLI

1. Connect keyboard / monitor to the TOE.
2. Enter a valid username and password to access the CLI.

NOTE: 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. Suppression of password entry is an automatic behavior that is not configured nor can it be modified.

7.1.3 Log in to Remote CLI

1. Open an SSH client and enter the IP address of the TOE then click “open”.
2. If using username and password to authenticate to the TOE, enter a valid username and password to access the CLI.

NOTE: If the using public key to authenticate then the public key will need to be selected in the SSH client prior to connection. Also, the SSH would need have been configured to use the public key per the configuration in Section 6.5 of this document.

7.2 Failed Authentication Lockout

The TSF provides a configurable counter for consecutive failed authentication attempts that will lock a user account when the failure counter threshold is reached. A valid login that happens prior to the failure counter reaching its threshold will reset the counter to zero. CLI user accounts are separate from Console user accounts, meaning a CLI user cannot log into the Console and vice versa.

The Console Security Administrator configures the number of failed attempts lockout threshold through the Console. The threshold can be set to a minimum of 1 and maximum of 10 consecutive failed attempts and applies to both the CLI and Console users. The default setting is 3 consecutive failed attempts.

The Console Security Administrator is also able to define a time period when locked Console accounts will automatically unlock. The default for this setting is 30 minutes for the Console. The lockout time period can be configured between 5-1000 minutes.

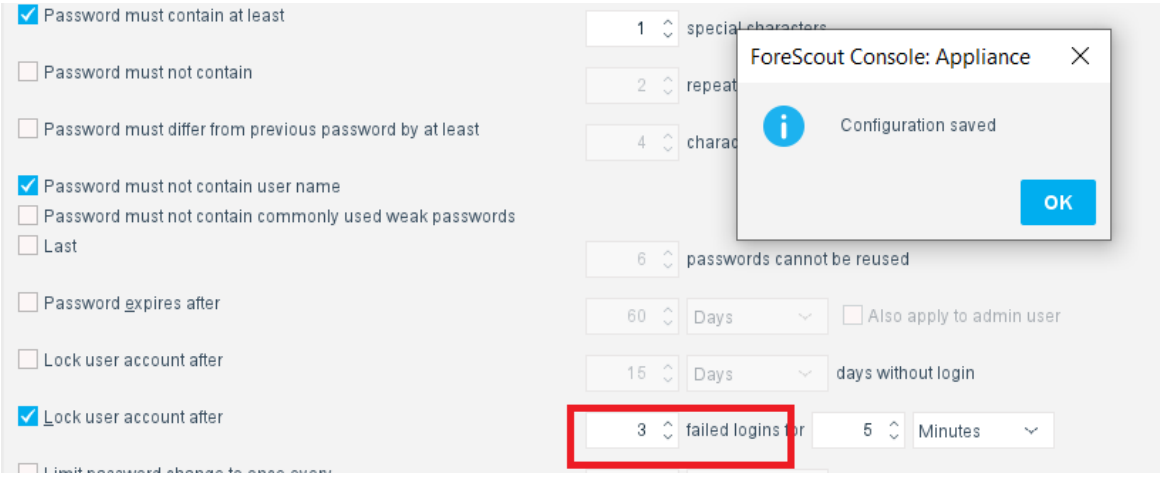
The CLI Security Administrator is able to define a time period when a locked CLI account will automatically unlock. The default for this setting is 24 hours for the CLI users. The lockout time period can be configured between 1-1000 minutes. Even though the TOE provides manual unlocking of locked accounts, it is recommended to only have a 3-5 minute lockout time period.

NOTE: Having multiple Security Administrator accounts (CLI and Console) that can be used to access the TOE remotely and/or locally to unlock other Security Administrator accounts mitigates a total lockout of the TOE.

7.2.1 Configuring Lockout Attributes

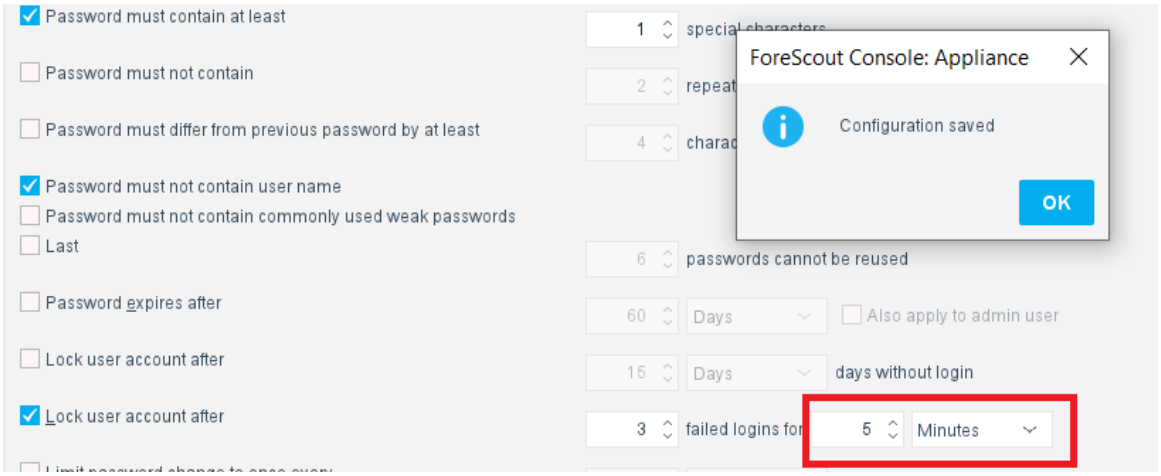
A Console Security Administrator can set the lockout attributes for all interfaces by performing the following steps:

1. Authenticate to the TOE via the Console using a Security Administrator account.
2. Navigate to “Tools” > “Options” > “CounterACT User Profiles” > “Password and Sessions”.
3. Select the “Password” tab.
4. Check the box, “Lock user account after” and set the inputs for “failed logins” and “minutes” to the desired values.
5. Select “Apply” and “OK” in the confirmation window.



NOTE: The number of failed logins threshold applies to both Console and CLI users.

The Console Security Administrator is also able to define the time period for when locked Console accounts will automatically unlock. The lockout time setting for Console accounts can be configured between 5-1000 minutes and this lockout time setting **only applies to the Console users.**



NOTE: The CLI lockout duration is configured and enforced independently from the Console.

```
cliadmin@fs4>fstool set_property os.lockout.fail 240
cliadmin@fs4>_
```

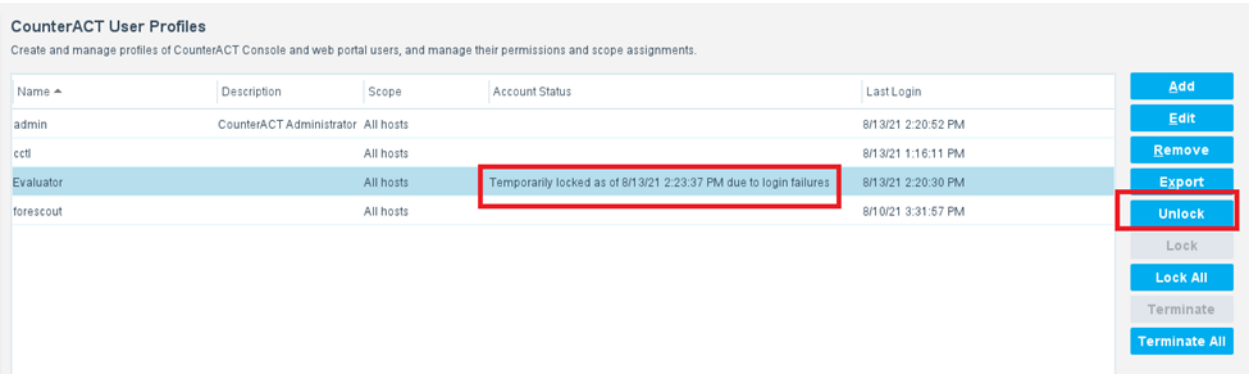
A CLI Security Administrator can set the time period for when locked CLI accounts will automatically unlock. The lockout time setting for the CLI accounts can be configured by a CLI Security Administrator via the command: "`fstool set_property os.lockout.fail <time in seconds>`" and this lockout time setting **only applies to CLI users.**

7.2.2 Manually Unlocking User Console Account From Console

For Console user accounts that are locked: A user with a locked account cannot login into the Console application until another Console Security Administrator manually unlocks the account via the Console or by a CLI Security Administrator.

A Console Security Administrator can unlock a Console user account by performing the following steps:

1. Authenticate to the TOE via the Console using a Security Administrator account.
2. Navigate to "Tools" > "Options" > "CounterACT User Profiles".
3. Click on the locked-out Console administrator or user account.
4. Click "Unlock".
5. Click "Yes" in the confirmation box.



NOTE: There is no functionality that allows a Console administrator to unlock a CLI user account.

7.2.3 Manually Unlocking User Console Account From CLI

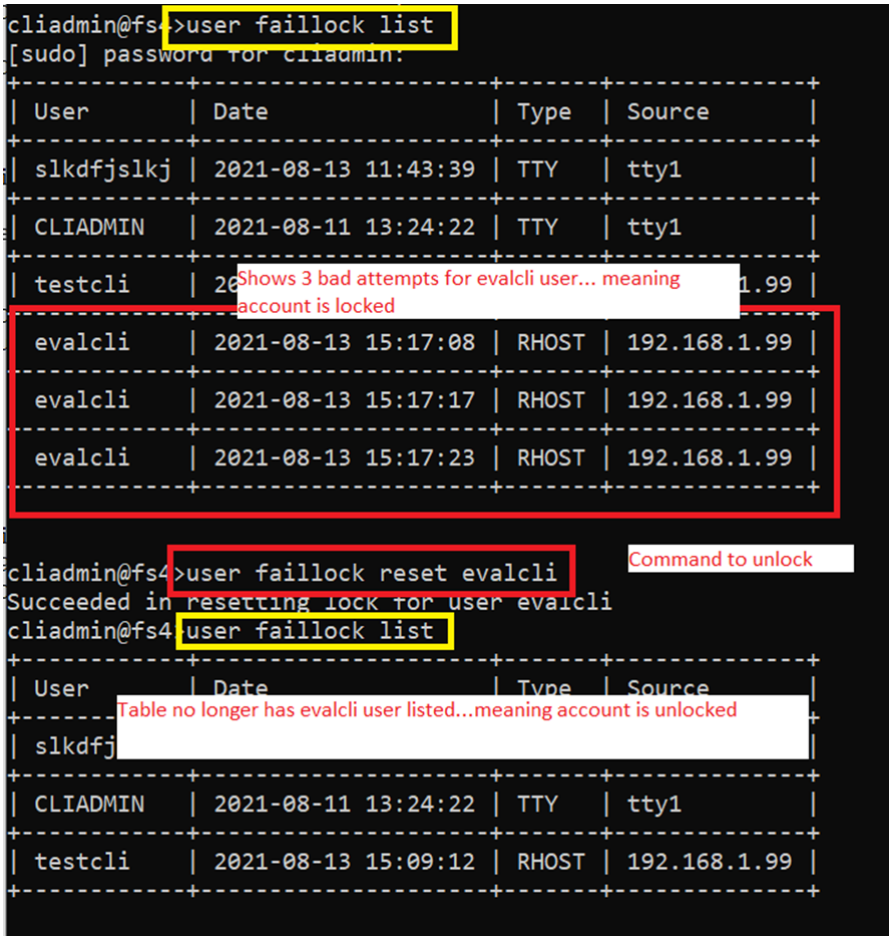
A CLI Security Administrator can unlock a Console user account by using the "`fstool unlock_console_user <user-id>`" command.

Note: This procedure can be used to unlock the default Console user 'admin' account when there are no other Console Security Administrator accounts.

7.2.4 Manually Unlocking CLI Account

For CLI user accounts that are locked: A user with a locked account cannot login to either the remote CLI or local console until a CLI Security Administrator manually unlocks the account using the "`user faillock reset <locked username>`" command or the configurable time limit has elapsed.

1. To list the current users with failures, execute the command: `user faillock list`
2. Verify the user account is locked out by appearing 3 times in the presented table
3. To unlock a specific user account, execute the command: `user faillock reset <username>`
4. The figure below is an output example when issuing the user `faillock` commands where the account is locked after 3 failed authentication attempts.



7.3 User Accounts and User Management

There are two types of user accounts, those that access the TOE through the CLI interfaces, and those that access through the Console. The TOE maintains the role of Security Administrator which is fulfilled by users with the "cliadmin" role assigned for the CLI interfaces and users assigned the "administrator" role for the Console by applying 'select all' permissions for the user account.

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 (role) 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 Console user assigned the TOE's "administrator" role has access to all Console tools and features and is able to administer the TOE remotely as a Security Administrator. All other Console users that do not have the full set of administrative permissions are categorized as a "Console User" and are not Security Administrators of the TOE.

The TOE has one predefined Console administrative user called "Admin". The "Admin" account is assigned the "administrator" role and these permissions cannot be modified or customized. A customized password must be created during installation by the customer. The "Admin" account is used to create additional Console Security Administrators.

A Console Security Administrator must assign permissions when creating any additional Console user. These permissions may be modified later by a Console Security Administrator. A Console User's set of permissions are customized by adding and subtracting specific permissions to allow/disallow the user TOE functionality. To create an additional Console Security Administrator, all the permissions must be selected and assigned to the user.

Additionally, the TOE has one predefined CLI administrative role called "cliadmin". CLI roles and permissions cannot be modified or customized at any time. A CLI Security Administrator is able to administer the TOE remotely via SSH or locally. A customized password must be created during installation by the customer. The "cliadmin" account is used to create additional CLI Security Administrators.

To create a Console user account, follow these steps:

1. Authenticate to the TOE via the Console using a Security Administrator account
2. Navigate to "Tools" > "Options" > "CounterACT User Profiles".
3. Select "Add". The Add User Profile wizard opens.
4. Navigate through the User Profile wizard to set the various user types and permissions (see the 'Creating Users and User Groups' section of the 'Managing Users' section in [2])
5. Click "Finish" to complete.
6. Select "Apply".

Permissions can also be configured after the user account is created by editing the account.

To create a cliadmin user account, follow these steps:

1. Authenticate to the TOE as a Security Administrator via the CLI.
2. Execute the "`fstool user add`" command.
3. Follow the interactive prompts to create the new user.
4. Specify the privilege as "CLI Admin".
5. Specify the password.

Permissions cannot be configured/altered for CLI users after the account is created.

For more information about creating user accounts and configuring them, The ‘Managing Users’ section in [2] describes the various permissions and managing local and external (e.g., Active Directory) user accounts.

7.4 Password Management

In the evaluated configuration, the TOE supports the ability for a Console Security Administrator to set the minimum password length to 15 characters or greater with a maximum of 30 characters. The accepted characters include upper- and lower-case letters, numbers, and the special characters “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”. In order to minimize the risk of account compromise, it is recommended to use a password that includes a mixture of uppercase, lowercase, numeric, and special characters and is not a common word or phrase, but is not so complex that it must be written down in order to be remembered.

The users are divided into two separate groups by how they access the TOE, whether through the Console or the CLI. An Security Administrator can set the minimum password for all interfaces to 15 characters by performing the following steps:

1. Authenticate to the TOE via the Console using a Security Administrator account.
2. Navigate to “Tools” > “Options” > “CounterACT User Profiles” > “Password and Sessions”.
3. Select the “Password” tab.
4. Define the “Minimum length” value to be 15.
5. Select “Apply”.

7.5 Login Banner

There are three possible ways to log in to the TOE: local CLI, remote CLI, and a remote Console. When logging in locally or remotely through any of the interfaces, a pre-authentication banner is displayed. It can be configured by a Console Security Administrator user via the Console.

1. Authenticate to the TOE via the Console using a Security Administrator account.
2. Navigate to “Tools” > “Options” > “CounterACT User Profiles” > “Password and Sessions”.
3. Select the “Login” tab.
4. Check the box, “Before login, prompt user to accept these Terms and Conditions,” and type a message in the adjacent text box.
5. Select “Apply”.

For more information on the configuring the banners, see the ‘Login Preferences’ section of the ‘Managing Users’ section in [2].

7.6 Session Termination

7.6.1 User Logout

A user accessing the TOE remotely or locally through the CLI can terminate their session by entering the ‘exit’ command. Users accessing the TOE remotely through the Console can terminate their session by clicking the “File” > “Log-Out” button.

7.6.2 Termination from Inactivity

The TOE is designed to terminate a local CLI (local console), remote CLI, and remote Console session after a given amount of time passes on the system clock. The timeout setting applies to both the local and remote CLI. The timeout period is defined in minutes for both the CLI and Console settings and configurable by a Console Security Administrator. The following steps can be performed to set the timeouts for all interfaces:

1. Authenticate to the TOE via the Console using a Security Administrator account.
2. Navigate to “Tools” > “Options” > “CounterACT User Profiles” > “Password and Sessions”.
3. Select the “Session” tab.
4. Check the box, “Terminate inactive sessions after”, and specify the value in minutes.
5. Select “Apply”.

7.7 System Time Configuration

The TOE has an underlying hardware clock that is used for time keeping. In the evaluated configuration of the TOE, the system time is expected to be manually set. A CLI Security Administrator user can configure all aspects of the clock using the local or remote CLI.

1. Authenticate to the TOE via the CLI using a Security Administrator account.
2. Execute the following command to set the date and time:

```
date -s "YYYY-MM-DD HH:MM:SS"

date --hwclock
```

7.8 Secure Updates

To maintain security throughout the lifecycle of the Forescout product, the TOE provides a mechanism to apply software updates. When an updated software image becomes available, a Security Administrator with a support account at https://www.forescout.com/support/login/ will receive an email or a Security Administrator can go to https://www.forescout.com/support/login/ to view available software image patches.

When an update is available, a 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 an updated software image is available and downloaded, the following procedures are performed to update the TOE to the updated version:

1. Place the software image on the Management Workstation
2. Authenticate to the TOE via the Console using a Security Administrator account
3. Obtain the current version of the TOE:
    a. Navigate to “Help” > “About Forescout”.

b. Navigate to “Tools” > “Options” > “Modules”.
c. Notate the version and build number.

4. Install the latest software image:
    a. Navigate to “Tools” > “Options” > and:
        i. If on an Enterprise Manager, select “CounterACT Devices”.
        ii. If on an Appliance, select “Appliance”.
    b. Click “Upgrade”.
    c. Specify the update file (e.g., service pack) and click “Install”.
    d. Once the update file has been fully uploaded, the TOE will verify the digital signature of the update file and:
        i. If the digital signature verification check is successful, the update process will continue and the next procedure to be followed is Step 5.
        ii. If the digital signature verification check is unsuccessful, the update process is halted:
            1. A warning banner will appear notifying the administrator of the failed attempt.
            2. The next procedure to be followed is Step 8.
5. Proceed through the dialog boxes of the wizard to install the update.
6. After an update finishes installing, the TOE will normally reboot.
7. If individual plugin files have been provided for update as well:
    a. Navigate to “Tools” > “Options” > “Modules” > “Install”.
    b. Specify the plugin update file.
8. Repeat Step 3 and:
    a. If the installation was successful, verify that the currently installed version corresponds to that of the update.
    b. If the installation was unsuccessful, verify that the currently installed version remains unchanged from the original execution of Step 3.

For more information on updating the TOE, see the ‘Managing Appliances, Enterprise Managers, and Consoles’ section in [2].

8 Auditing

In order to be compliant with Common Criteria, the TOE audits the events in the table below. Performing the steps in Sections 6.6 and 6.7 of this document are all the steps required for the TOE to generate the required audit records, store them locally, and send them to a remote audit server.

The following is an example of an audit record that Forescout produces:

> 2021-08-09T15:25:22-04:00 localhost fs4 sshd[70759]: Connection from 192.168.1.99 port 58398 on 192.168.1.168 port 22
>
> 2021-08-09T15:25:26-04:00 localhost fs4 sshd[70759]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.99 user=cliadmin

2021-08-09T15:25:26-04:00 localhost fs4 sshd[70759]: pam_radius_auth: Could not open configuration file /etc/raddb/server: No such file or directory

2021-08-09T15:25:31-04:00 localhost fs4 sshd[70759]: Failed password for cliadmin from 192.168.1.99 port 58398 ssh2

Each audit record contains identifying information required by Common Criteria including the date and time the event occurred (2021-08-09T15:25:26-04:00), the type of event (authentication failure), the subject identity of the event (user=cliadmin), and the outcome of the event (failure).

Sample audit records for each security-relevant auditable event are included in the following table.

Auditable Event	Sample Audit Record
Start-up and shut-down of the audit functions	**Shutdown of audit (synonymous with shutdown of TOE):** 2021-08-30T12:52:12-04:00 localhost fs4 systemd: Stopping System Logging Service... 2021-08-30T12:52:12-04:00 localhost fs4 rsyslogd: [origin software="rsyslogd" swVersion="8.24.0-52.el7" x-pid="2181" x-info="http://www.rsyslog.com"] exiting on signal 15. 2021-08-30T12:52:12-04:00 localhost fs4 systemd: Stopped System Logging Service. **Startup of audit (synonymous with startup of TOE):** 2021-08-30T12:52:12-04:00 localhost fs4 systemd: Starting System Logging Service... 2021-08-30T12:52:12-04:00 localhost fs4 rsyslogd: [origin software="rsyslogd" swVersion="8.24.0-52.el7" x-pid="3677" x-info="http://www.rsyslog.com"] start 2021-08-30T12:52:12-04:00 localhost fs4 systemd: Started System Logging Service. 2021-08-30T12:52:12-04:00 localhost fs4 ipmievd: Waiting for events...
Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).	Refer to the ‘All uses of the authentication mechanism’ row in this table
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).	Refer to the ‘All management activities of the TSF’ row in this table
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).	Refer to the ‘All management activities of the TSF’ row in this table

Resetting passwords (name of related user account shall be logged).	**Console:** 2021-08-10T16:03:31-04:00 localhost fs4 fs4[60200]: User cctl session 1461665409753932449 changed Configuration. Details: User 'cctl' changed their password. **CLI:** 2021-08-10T17:27:20-04:00 localhost fs4 fs-cli[139520]: User testcli session 192.168.1.99 63418 22 executed command: password : Status succeeded
Failure to establish an SSH session	**SSH session failure (authentication failure):** 2021-07-15T13:02:23-04:00 fs4 sshd[87090]: Connection from 192.168.1.98 port 50179 on 192.168.1.168 port 22 2021-07-15T13:02:25-04:00 fs4 sshd[87090]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.98 user=cliadmin **SSH session failure (integrity check failure):** 2021-07-15T13:11:39-04:00 fs4 fs4[84887]: User cliadmin session 0 changed Authentication. Details: session opened for user cliadmin 2021-07-15T13:11:39-04:00 fs4 sshd[90779]: Starting session: command for cliadmin from 192.168.1.179 port 58408 id 0 2021-07-15T13:11:40-04:00 fs4 sshd[90779]: Bad packet length 1097756. 2021-07-15T13:11:40-04:00 fs4 sshd[90779]: ssh_dispatch_run_fatal: Connection from 192.168.1.179 port 58408: message authentication code incorrect 2021-07-15T13:11:40-04:00 fs4 sshd[90755]: pam_unix(sshd:session): session closed for user cliadmin **SSH session failure (mismatched algorithm):** 2021-07-15T13:05:30-04:00 fs4 sshd[87931]: Connection from 192.168.1.98 port 50181 on 192.168.1.168 port 22 2021-07-15T13:05:30-04:00 fs4 sshd[87931]: Unable to negotiate with 192.168.1.98 port 50181: no matching host key type found. Their offer: ssh-dss [preauth] 2021-07-15T13:08:43-04:00 fs4 sshd[88973]: Connection from 192.168.1.98 port 50185 on 192.168.1.168 port 22 2021-07-15T13:08:43-04:00 fs4 sshd[88973]: Unable to negotiate with 192.168.1.98 port 50185: no matching MAC found. Their offer: hmac-md5 [preauth]

	2021-07-15T13:09:52-04:00 fs4 sshd[89244]: Connection from 192.168.1.98 port 50186 on 192.168.1.168 port 22 2021-07-15T13:09:52-04:00 fs4 sshd[89244]: Unable to negotiate with 192.168.1.98 port 50186: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1,ext-info-c [preauth]
Failure to establish a TLS session	**TLS Client (mismatched version):** 2021-11-02T11:34:34-04:00 localhost fs4 fs4[2877]: Log: User Directory Connect Error. Details: [192.168.1.168] [ldaps://WINSRV2012R2-01.catl.local:636][negotiate] Connect Failed [SSL connect attempt failed error:1409210A:SSL routines:ssl3_get_server_hello:wrong ssl version]. Severity: 3 **TLS Server (mismatched ciphersuite):** 2021-08-16T12:10:05-04:00 localhost fs4 fs4[88707]: Log: Failed to negotiate SSL cipher suite for connection from 192.168.1.98, host name 192.168.1.98. Details: Failed to negotiate SSL cipher suite for connection from 192.168.1.98, host name 192.168.1.98. Severity: 3
Unsuccessful login attempts limit is met or exceeded	**CLI:** 2021-08-09T15:25:22-04:00 localhost fs4 sshd[70759]: Connection from 192.168.1.99 port 58398 on 192.168.1.168 port 22 2021-08-09T15:25:26-04:00 localhost fs4 sshd[70759]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.99 user=cliadmin 2021-08-09T15:25:31-04:00 localhost fs4 sshd[70759]: Failed password for cliadmin from 192.168.1.99 port 58398 ssh2 2021-08-09T15:25:32-04:00 localhost fs4 sshd[70759]: pam_faillock(sshd:auth): Consecutive login failures for user cliadmin account temporarily locked **Console:** 2021-08-09T14:40:14-04:00 localhost fs4 fs4[49710]: Log: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Details: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Severity: 6 2021-08-09T14:40:14-04:00 localhost fs4 fs4[49710]: User admin session 0 changed Enterprise Manager Console. Details: User 'admin' at host IP 192.168.1.99 attempted to log in to Enterprise Manager 192.168.1.168: Login failed: Failed to authenticate user 2021-08-09T14:40:14-04:00 localhost fs4 fs4[49710]: Log: Login failed admin@192.168.1.99. Details: User admin failed to login from 192.168.1.99. Severity: 4 2021-08-09T14:40:15-04:00 localhost fs4 fs4[49710]: User Evaluator session 0 changed Enterprise Manager Console. Details: Failed to login from 192.168.1.99 as Evaluator for 3 times; account will be locked for 5 minutes

All uses of the authentication mechanism	**Successful Console authentication with AD:** 2021-08-09T14:29:38-04:00 localhost fs4 fs4[49710]: Log: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Details: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Severity: 6 2021-08-09T14:29:39-04:00 localhost fs4 fs4[49710]: Log: User Directory Login Successful. Details: [192.168.1.168] [ldaps://WINSRV2012R2-01.catl.local:636][tlsv1_2] [forescout@catl.local] Login Successful.. Severity: 6 2021-08-09T14:29:39-04:00 localhost fs4 fs4[49710]: Log: User Directory Disconnect Successful. Details: [192.168.1.168] [ldaps://WINSRV2012R2-01.catl.local:636][forescout@catl.local] Disconnect Successful.. Severity: 6 2021-08-09T14:29:39-04:00 localhost fs4 fs4[49710]: Log: Login success by forescout@192.168.1.99. Details: User forescout logged in from 192.168.1.99. Severity: 6 2021-08-09T14:29:39-04:00 localhost fs4 fs4[49710]: User forescout session 0 changed Enterprise Manager Console. Details: User 'forescout' at host IP 192.168.1.99 attempted to log in to Enterprise Manager 192.168.1.168: Login succeeded<EOL> 3 successful login(s) in the last 60 days. **Failed Console authentication with AD:** 2021-08-09T14:31:40-04:00 localhost fs4 fs4[49710]: Log: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Details: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Severity: 6 2021-08-09T14:31:41-04:00 localhost fs4 fs4[49710]: Log: User Directory Login Error. Details: [192.168.1.168] [3334: ldaps://WINSRV2012R2-01.catl.local:636][tlsv1_2] [forescout@catl.local] Login Failed [80090308: LdapErr: DSID-0C09042F, comment: AcceptSecurityContext error, data 52e, v2580]. Severity: 3 2021-08-09T14:31:41-04:00 localhost fs4 fs4[49710]: Log: User Directory Disconnect Successful. Details: [192.168.1.168] [ldaps://WINSRV2012R2-01.catl.local:636][forescout@catl.local] Disconnect Successful.. Severity: 6 2021-08-09T14:31:41-04:00 localhost fs4 fs4[49710]: User forescout session 0 changed Enterprise Manager Console. Details: User 'forescout' at host IP 192.168.1.99 attempted to log in to Enterprise Manager 192.168.1.168: Login failed: Failed to authenticate user 2021-08-09T14:31:41-04:00 localhost fs4 fs4[49710]: Log: Login failed forescout@192.168.1.99. Details: User forescout failed to login from 192.168.1.99. Severity: 4 **Successful Console authentication no AD:** 2021-08-06T16:41:58-04:00 localhost fs4 fs4[49710]: Log: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Details: Loaded

	ConfigParams: FSAllowedConsoleAddressesParams. Severity: 62021-08-06T16:41:59-04:00 localhost fs4 fs4[49710]: Log: Login success by admin@192.168.1.99. Details: User admin logged in from 192.168.1.99. Severity: 6 2021-08-06T16:41:59-04:00 localhost fs4 fs4[49710]: User admin session 0 changed Enterprise Manager Console. Details: User 'admin' at host IP 192.168.1.99 attempted to log in to Enterprise Manager 192.168.1.168: Login succeeded<EOL> 5 successful login(s) in the last 60 days. 2021-08-06T16:42:26-04:00 localhost fs4 fs4[49710]: User admin session 2352418089700637963 changed . Details: Successful accesses to 192.168.1.168 host details **Failed Console authentication no AD:** 2021-08-09T14:40:14-04:00 localhost fs4 fs4[49710]: Log: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Details: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Severity: 6 2021-08-09T14:40:14-04:00 localhost fs4 fs4[49710]: User admin session 0 changed Enterprise Manager Console. Details: User 'admin' at host IP 192.168.1.99 attempted to log in to Enterprise Manager 192.168.1.168: Login failed: Failed to authenticate user 2021-08-09T14:40:14-04:00 localhost fs4 fs4[49710]: Log: Login failed admin@192.168.1.99. Details: User admin failed to login from 192.168.1.99. Severity: 4 **Successful SSH CLI authentication using username/password:** 2021-08-06T16:36:18-04:00 localhost fs4 fs4[49710]: User cliadmin session 0 changed Authentication. Details: 192.168.1.99 port 60037 ssh2 2021-08-06T16:36:18-04:00 localhost fs4 systemd: Created slice User Slice of cliadmin. 2021-08-06T16:36:18-04:00 localhost fs4 systemd: Started Session 18 of user cliadmin. 2021-08-06T16:36:19-04:00 localhost fs4 fs4[49710]: User cliadmin session 0 changed Authentication. Details: session opened for user cliadmin **Failed SSH CLI authentication using username/password:** 2021-08-09T15:25:22-04:00 localhost fs4 sshd[70759]: Connection from 192.168.1.99 port 58398 on 192.168.1.168 port 22 2021-08-09T15:25:26-04:00 localhost fs4 sshd[70759]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.99 user=cliadmin 2021-08-09T15:25:31-04:00 localhost fs4 sshd[70759]: Failed password for cliadmin from 192.168.1.99 port 58398 ssh2

	Successful SSH CLI using Public Key: 2021-09-02T11:29:49-04:00 localhost fs4 sshd[7584]: Connection from 192.168.1.99 port 64614 on 192.168.1.168 port 22 2021-09-02T11:29:55-04:00 localhost fs4 fs-cli[7592]: Request authentication key for user cliadmin session local. 2021-09-02T11:29:55-04:00 localhost fs4 sshd[7584]: Accepted publickey for cliadmin from 192.168.1.99 port 64614 ssh2: RSA SHA256:LA87XVAYMGtPeyqcpkq58zBRQY+si9ENWFyf5AQYZfo 2021-09-02T11:29:55-04:00 localhost fs4 fs4[130830]: User cliadmin session 0 changed Authentication. Details: 192.168.1.99 port 64614 ssh2: RSA SHA256:LA87XVAYMGtPeyqcpkq58zBRQY+si9ENWFyf5AQYZfo 2021-09-02T11:29:55-04:00 localhost fs4 systemd-logind: New session 576 of user cliadmin. 2021-09-02T11:29:55-04:00 localhost fs4 sshd[7584]: pam_unix(sshd:session): session opened for user cliadmin by (uid=0) **Failed SSH CLI using Public Key:** 2021-09-02T11:37:23-04:00 localhost fs4 sshd[11135]: Connection from 192.168.1.99 port 64650 on 192.168.1.168 port 22 2021-09-02T11:37:24-04:00 localhost fs4 fs-cli[11138]: Request authentication key for user cliadmin session local. 2021-09-02T11:37:24-04:00 localhost fs4 sshd[11135]: Failed publickey for cliadmin from 192.168.1.99 port 64650 ssh2: RSA SHA256:XvuKO4SUHXC8trexZnOaR0FQvwWkdQs6UUQMAGH9uRA **Successful Local CLI authentication:** 2021-08-06T16:57:03-04:00 localhost fs4 kernel: usb 1-1.6.1: new high-speed USB device number 6 using ehci-pci 2021-08-06T16:57:03-04:00 localhost fs4 kernel: usb 1-1.6.1: New USB device found, idVendor=0624, idProduct=0249 2021-08-06T16:57:03-04:00 localhost fs4 kernel: usb 1-1.6.1: New USB device strings: Mfr=4, Product=5, SerialNumber=6 2021-08-06T16:57:03-04:00 localhost fs4 kernel: usb 1-1.6.1: Product: Keyboard/Mouse Function 2021-08-06T16:57:03-04:00 localhost fs4 kernel: usb 1-1.6.1: Manufacturer: Avocent 2021-08-06T16:57:03-04:00 localhost fs4 kernel: usb 1-1.6.1: SerialNumber: 20121018 2021-08-06T16:57:03-04:00 localhost fs4 kernel: input: Avocent Keyboard/Mouse Function as /devices/pci0000:00/0000:00:1a.0/usb1/1-1/1-1.6/1-1.6.1/1-1.6.1:1.0/0003:0624:0249.0006/input/input7

	2021-08-06T16:57:03-04:00 localhost fs4 kernel: hid-generic 0003:0624:0249.0006: input,hidraw2: USB HID v1.00 Keyboard [Avocent Keyboard/Mouse Function] on usb-0000:00:1a.0-1.6.1/input0 2021-08-06T16:57:03-04:00 localhost fs4 kernel: input: Avocent Keyboard/Mouse Function as /devices/pci0000:00/0000:00:1a.0/usb1/1-1/1-1.6/1-1.6.1/1-1.6.1:1.1/0003:0624:0249.0007/input/input8 2021-08-06T16:57:03-04:00 localhost fs4 kernel: hid-generic 0003:0624:0249.0007: input,hidraw3: USB HID v1.00 Mouse [Avocent Keyboard/Mouse Function] on usb-0000:00:1a.0-1.6.1/input1 2021-08-06T16:57:03-04:00 localhost fs4 kernel: input: Avocent Keyboard/Mouse Function as /devices/pci0000:00/0000:00:1a.0/usb1/1-1/1-1.6/1-1.6.1/1-1.6.1:1.2/0003:0624:0249.0008/input/input9 2021-08-06T16:57:03-04:00 localhost fs4 kernel: hid-generic 0003:0624:0249.0008: input,hidraw4: USB HID v1.00 Mouse [Avocent Keyboard/Mouse Function] on usb-0000:00:1a.0-1.6.1/input2 2021-08-06T16:57:29-04:00 localhost fs4 systemd: Created slice User Slice of cliadmin. 2021-08-06T16:57:29-04:00 localhost fs4 systemd: Started Session 24 of user cliadmin. 2021-08-06T16:57:29-04:00 localhost fs4 systemd: Started Session 24 of user cliadmin. 2021-08-06T16:57:29-04:00 localhost fs4 login: pam_unix(login:session): session opened for user cliadmin by LOGIN(uid=0) 2021-08-06T16:57:29-04:00 localhost fs4 login: LOGIN ON tty1 BY cliadmin **Failed Local CLI authentication:** 2021-08-09T15:51:04-04:00 localhost fs4 login: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1 ruser= rhost= user=cliadmin 2021-08-09T15:51:04-04:00 localhost fs4 login: pam_radius_auth: Could not open configuration file /etc/raddb/server: No such file or directory 2021-08-09T15:51:05-04:00 localhost fs4 login: FAILED LOGIN SESSION FROM tty1 FOR cliadmin, Permission denied
Unsuccessful attempt to validate a certificate	2021-11-02T10:21:20-04:00 localhost fs4 fs4[136950]: Log: User Directory Connect Error. Details: [192.168.1.168] [ldaps://WINSRV2012R2-01.catl.local:636][negotiate] Connect Failed [http://192.168.1.3:8888: certificate status is revoked; subject: /C=US/ST=Maryland/L=Laurel/O=BAH/OU=CCTL/CN=WINSRV2012R2-01.catl.local]. Severity: 3
Any attempt to initiate a manual update	**Successful attempt using just "Upload only" functions:** 2021-08-25T09:47:07-04:00 localhost fs4 fs4[138958]: User admin session 9211121023334655609 changed Software Upgrade. Details:

	Upload of upgrade file CounterACT-8.3.0-132_Upgrade_from_8.1.1-61_upward.fsp initiated by user. **Successful attempt using "Upgrade" only function (you can only run against a successfully uploaded file which has already passed digital signature verification):** 2021-08-26T16:15:26-04:00 localhost fs4 fs4[2842]: User admin session 9211121023334655609 changed Software Upgrade. Details: Installation of upgrade file CounterACT-8.3.0-132_Upgrade_from_8.1.1-61_upward.zip initiated by user. **Successful attempts using "Upload and Upgrade" function:** 2021-08-27T09:20:22-04:00 localhost fs4 fs4[2842]: User admin session 8990149723673553347 changed Software Upgrade. Details: Installation of upgrade file CounterACT-8.3.0-132_Upgrade_from_8.1.1-61_upward.zip initiated by user. 2021-08-27T09:22:14-04:00 localhost fs4 fs4[2842]: User admin session 8990149723673553347 changed Software Upgrade. Details: CounterACT upgraded to version 8.3.0
All management activities of the TSF	**FTA_TAB.1 Audit for configuring Warning Banner:** 2021-08-06T15:57:29-04:00 localhost fs4 fs4[49710]: User admin session 6639665725833569959 changed Password and Sessions. Details: Before login, prompt user to accept these Terms and Conditions requirement: Previous Value: Disabled; Current Value: Enabled <EOL> Before login, prompt user to accept these Terms and Conditions value: Previous Value: ; Current Value: This is a warning banner that must be accepted. **FTA_SSL.3 Audit for configuring session inactivity timer:** 2021-08-11T13:39:44-04:00 localhost fs4 fs4[123470]: User admin session 7487640271386897280 changed Password and Sessions. Details: Terminate inactive sessions after value: Previous Value: 4 minutes; Current Value: 5 minutes **FPT_TUD_EXT.1 Initiation of update (success and failure):** 2021-12-22T10:23:42-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward.fsp initiated by user. **Successful update:** 2021-12-22T10:25:48-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: CounterACT upgraded to version 8.3.0.1 **Invalid binary (hexedit):**

	2021-12-22T10:19:28-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_hexedit_binary.fsp initiated by user. 2021-12-22T10:19:34-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of unsigned upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_hexedit_binary.fsp blocked. **Missing signature:** 2021-12-22T10:20:30-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_no_signature.fsp initiated by user. 2021-12-22T10:20:30-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of unsigned upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_no_signature.fsp blocked. **Invalid signature:** 2021-12-22T10:21:20-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_invalid_signature.fsp initiated by user. 2021-12-22T10:21:22-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of unsigned upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_invalid_signature.fsp blocked. **FIA_AFL/Console Audit for configuring lock out time for Console accounts and number of failed attempts that applies to both Console and CLI accounts:** 2021-08-11T15:24:07-04:00 localhost fs4 fs4[123470]: User admin session 7862653848401784581 changed Password and Sessions. Details: Password expires after value: Previous Value: 2 password failures for 5 minutes ; Current Value: 3 password failures for 5 minutes **FIA_AFL/CLI Audit for configuring lock out time for CLI Accounts:** 2021-08-18T17:31:19-04:00 localhost fs4 fs4[145958]: User root session 0 changed Configuration. Details: setting property: os.lockout.fail with value: 240 2021-08-18T17:31:19-04:00 localhost fs4 fs-cli[21737]: User cliadmin session local executed command: set_property os.lockout.fail 240: Status succeeded 2021-08-18T17:31:19-04:00 localhost fs4 fs4[145958]: User Syslog plugin session 0 changed Configuration. Details: User cliadmin session local executed command: set_property os.lockout.fail 240: Status succeeded

	FIA_AFL.1/ Audit for manual release of locked Console account: 2021-08-13T14:24:35-04:00 localhost fs4 fs4[88707]: Log: Account Evaluator released by administrator.. Details: Account Evaluator released by administrator.. Severity: 6 2021-08-13T14:24:35-04:00 localhost fs4 fs4[88707]: User admin session 4346647647062219404 changed User Management. Details: User Evaluator was released by user admin **FIA_AFL/CLI Audit for manual release of locked CLI account:** 2021-08-13T15:09:09-04:00 localhost fs4 fs-cli[120602]: User cliadmin session 192.168.1.99 57521 22 executed command: user faillock reset evalcli: Status succeeded 2021-08-13T15:09:09-04:00 localhost fs4 fs4[88707]: User Syslog plugin session 0 changed Configuration. Details: User cliadmin session 192.168.1.99 57521 22 executed command: user faillock reset evalcli: Status succeeded **FCS_SSHS_EXT.1.8 Audit for configuring Rekey Parameters:** 2021-09-08T14:04:12-04:00 localhost fs4 fs-cli[136619]: User evalcli session 192.168.1.99 63112 22 executed command: ssh -t server -o RekeyLimit 1G 1h: Status succeeded 2021-09-08T14:04:12-04:00 localhost fs4 fs4[136950]: User Syslog plugin session 0 changed Configuration. Details: User evalcli session 192.168.1.99 63112 22 executed command: ssh -t server -o RekeyLimit 1G 1h: Status succeeded **FMT_SMF.1 Audit for Syslog Configuration** 2022-03-01T14:31:11-05:00 fs5 fs5[6751]: User admin session 851326545588027266 changed Syslog Configuration. Details: Edited the following CounterACT Appliance: :<EOL> Edited the following Send messages triggered by events to all of the following Syslog servers. Each message includes the Message Identity and the Priority (Facility and Severity) defined below. :<EOL> Soft-fail OCSP requests 1: Previous Value: false; Current Value: true 2022-03-28T13:28:45-04:00 fs5 fs5[21568]: User admin session 3551246059627668414 changed Syslog Configuration. Details: Edited the following CounterACT Appliance: :<EOL> Include operating system messages: Previous Value: false; Current Value: true 2022-03-28T13:29:39-04:00 fs5 fs5[21864]: User admin session 3551246059627668414 changed Syslog Configuration. Details: Edited the following CounterACT Appliance: :<EOL> Server Protocol: Previous Value: udp; Current Value: tcp 2022-03-29T12:26:01-04:00 fs5 fs5[29302]: User admin session 2387039897880016747 changed Syslog Configuration. Details: Edited the

	following CounterACT Appliance: :<EOL> Server Port: Previous Value: 514; Current Value: 6514 <EOL> Message Identity: Previous Value: CounterACT; Current Value: fs5 <EOL> Include operating system messages: Previous Value: false; Current Value: true <EOL> Server Protocol: Previous Value: udp; Current Value: tcp <EOL> Server Address: Previous Value: ; Current Value: syslog04.catl.local <EOL> Severity: Previous Value: info; Current Value: debug <EOL> <EOL> Added the following Send messages triggered by events to all of the following Syslog servers. Each message includes the Message Identity and the Priority (Facility and Severity) defined below.:<EOL> Server Address 1: syslog04.catl.local <EOL> Server Port 1: 6514 <EOL> Server Protocol 1: tcp <EOL> Use TLS 1: true <EOL> Soft-fail OCSP requests 1: true <EOL> Identity 1: fs5 <EOL> Facility 1: local4 <EOL> Severity 1: debug **FMT_PMG_EXT.1 Audit for configuring password length:** 2021-08-10T15:49:58-04:00 localhost fs4 fs4[60200]: User forescout session 8957396401568145289 changed Password and Sessions. Details: Minimum length number: Previous Value: 11; Current Value: 15 **FPT_STM_EXT.1 Audit for Setting Time:** 2021-08-30T14:05:00-04:00 localhost fs4 fs-cli[53818]: System time change from: 'Mon Aug 30 14:04:27 2021 (EDT)' to: 'Mon Aug 30 14:05:00 2021 (EDT)' 2021-08-30T14:05:00-04:00 localhost fs4 fs4[23383]: User Syslog plugin session 0 changed Configuration. Details: System time change from: 'Mon Aug 30 14:04:27 2021 (EDT)' to: 'Mon Aug 30 14:05:00 2021 (EDT)' 2021-08-30T14:05:00-04:00 localhost fs4 fs-cli[23031]: User evalcli session 192.168.1.99 60347 22 executed command: date -s 2021-08-30 14:05:00: Status succeeded 2021-08-30T14:05:00-04:00 localhost fs4 fs4[23383]: User Syslog plugin session 0 changed Configuration. Details: User evalcli session 192.168.1.99 60347 22 executed command: date -s 2021-08-30 14:05:00: Status succeeded 2021-08-30T14:05:07-04:00 localhost fs4 fs-cli[23031]: User evalcli session 192.168.1.99 60347 22 executed command: date --hwclock: Status succeeded 2021-08-30T14:05:07-04:00 localhost fs4 fs4[23383]: User Syslog plugin session 0 changed Configuration. Details: User evalcli session 192.168.1.99 60347 22 executed command: date --hwclock: Status succeeded **FCS_SSH_EXT.1 Audit for configuring Public Key authentication:** 2021-09-07T15:52:40-04:00 localhost fs4 fs4[141637]: User Syslog plugin session 0 changed Configuration. Details: User evalcli session 192.168.1.99 63097 22 executed command: user auth setkey: Status failed

	2021-09-07T15:53:03-04:00 localhost fs4 fs4[141637]: User Syslog plugin session 0 changed Configuration. Details: User evalcli session 192.168.1.99 63097 22 executed command: user auth setkey: Status succeeded 2021-09-07T15:55:39-04:00 localhost fs4 fs4[141637]: User Syslog plugin session 0 changed Configuration. Details: User evalcli session 192.168.1.99 63097 22 executed command: user auth rmkey: Status succeeded **Audit for configuring Trust Store:** 2021-09-07T14:55:53-04:00 localhost fs4 fs4[141637]: User admin session 4746463605633018989 changed Configuration. Details: Change trusted certificates configuration definition to <EOL> <EOL> Added: FingerPrint 'a932890176fc57cf959bcc32fa419c6828689619' Issued to 'CCTL Root CA' Issued by 'CCTL Root CA'<EOL> Status enabled;Trusted For All subsystems on All devices;<EOL> Removed: FingerPrint 'a932890176fc57cf959bcc32fa419c6828689619' Issued to 'CCTL Root CA' Issued by 'CCTL Root CA'<EOL> Status enabled;Trusted For All subsystems on All devices; 2021-09-07T14:58:09-04:00 localhost fs4 fs4[141637]: User admin session 4746463605633018989 changed Configuration. Details: Change trusted certificates configuration definition to <EOL> <EOL> Added: FingerPrint 'a932890176fc57cf959bcc32fa419c6828689619' Issued to 'CCTL Root CA' Issued by 'CCTL Root CA'<EOL> Status enabled;Trusted For All subsystems on All devices; 2021-09-07T14:57:48-04:00 localhost fs4 fs4[141637]: User admin session 4746463605633018989 changed Configuration. Details: Change trusted certificates configuration definition to <EOL> <EOL> Removed: FingerPrint 'a932890176fc57cf959bcc32fa419c6828689619' Issued to 'CCTL Root CA' Issued by 'CCTL Root CA'<EOL> Status enabled;Trusted For All subsystems on All devices;
Discontinuous changes to time - either Administrator actuated or changed via an automated process.	2021-08-30T14:05:00-04:00 localhost fs4 fs-cli[53818]: System time change from: 'Mon Aug 30 14:04:27 2021 (EDT)' to: 'Mon Aug 30 14:05:00 2021 (EDT)'
Initiation of update; result of the update attempt (success or failure)	**FPT_TUD_EXT.1 Initiation of update (success and failure):** 2021-12-22T10:23:42-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward.fsp initiated by user. **Successful update:** 2021-12-22T10:25:48-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: CounterACT upgraded to version 8.3.0.1 **Invalid binary (hexedit):** 2021-12-22T10:19:28-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details:

	Installation of upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_hexedit_binary.fsp initiated by user. 2021-12-22T10:19:34-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of unsigned upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_hexedit_binary.fsp blocked. **Missing signature:** 2021-12-22T10:20:30-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_no_signature.fsp initiated by user. 2021-12-22T10:20:30-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of unsigned upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_no_signature.fsp blocked. **Invalid signature:** 2021-12-22T10:21:20-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_invalid_signature.fsp initiated by user. 2021-12-22T10:21:22-05:00 localhost fs6 fs6[26025]: User admin session 4254021658832139723 changed Software Upgrade. Details: Installation of unsigned upgrade file CounterACT-8.3.0.1-72_Upgrade_from_8.3.0-233_upward_invalid_signature.fsp blocked.
The termination of a local session by the session locking mechanism.	**Local CLI Session:** 2021-08-11T13:20:30-04:00 localhost fs4 fs-cli[84750]: Session timed out. 2021-08-11T13:20:30-04:00 localhost fs4 fs4[123470]: User Syslog plugin session 0 changed Authentication. Details: Session timed out. 2021-08-11T13:20:30-04:00 localhost fs4 systemd: getty@tty1.service has no holdoff time, scheduling restart. 2021-08-11T13:20:30-04:00 localhost fs4 systemd: Stopped Getty on tty1. 2021-08-11T13:20:30-04:00 localhost fs4 systemd: Started Getty on tty1. 2021-08-11T13:20:30-04:00 localhost fs4 systemd-logind: Removed session 984.
The termination of a remote session by the session locking mechanism.	**Remote CLI Session:** 2021-08-11T13:02:49-04:00 localhost fs4 fs-cli[76737]: Session timed out. 2021-08-11T13:02:49-04:00 localhost fs4 fs4[123470]: User Syslog plugin session 0 changed Authentication. Details: Session timed out. 2021-08-11T13:02:50-04:00 localhost fs4 sshd[76736]: Close session: user cliadmin from 192.168.1.99 port 63032 id 0

	Console Session: 2021-08-11T11:43:39-04:00 localhost fs4 fs4[123470]: User admin session 7957762336569107831 changed Enterprise Manager Console. Details: CounterACT 192.168.1.168 terminated inactive session with host at 192.168.1.99
The termination of an interactive session	**Local CLI Session:** 2021-08-06T16:57:34-04:00 localhost fs4 login: pam_unix(login:session): session closed for user cliadmin 2021-08-06T16:57:34-04:00 localhost fs4 systemd: getty@tty1.service has no holdoff time, scheduling restart. 2021-08-06T16:57:34-04:00 localhost fs4 systemd: Stopped Getty on tty1. 2021-08-06T16:57:34-04:00 localhost fs4 systemd: Started Getty on tty1. 2021-08-06T16:57:34-04:00 localhost fs4 systemd-logind: Removed session 24. 2021-08-06T16:57:34-04:00 localhost fs4 systemd: Removed slice User Slice of cliadmin. **SSH CLI Session:** 2021-08-06T16:37:31-04:00 localhost fs4 sshd[72574]: Received disconnect from 192.168.1.99 port 60037:11: FlowSshClientSession: disconnected on user's request 2021-08-06T16:37:31-04:00 localhost fs4 sshd[72574]: Closing connection to 192.168.1.99 port 60037 2021-08-06T16:37:31-04:00 localhost fs4 sshd[72547]: pam_unix(sshd:session): session closed for user cliadmin 2021-08-06T16:37:31-04:00 localhost fs4 systemd-logind: Removed session 18. 2021-08-06T16:37:31-04:00 localhost fs4 fs4[49710]: User cliadmin session 0 changed Authentication. Details: session closed for user cliadmin 2021-08-06T16:37:31-04:00 localhost fs4 systemd: Removed slice User Slice of cliadmin **Console Session:** 2021-08-06T16:42:36-04:00 localhost fs4 fs4[49710]: Log: Logout by admin@192.168.1.99. Details: User admin@192.168.1.99 logged out. Severity: 6 2021-08-06T16:42:36-04:00 localhost fs4 fs4[49710]: User admin session 2352418089700637963 changed Enterprise Manager Console. Details: Logout from 192.168.1.168 by host 192.168.1.99 : Logout succeeded

Initiation of the trusted channel	**TLS audit server:** 2021-08-30T16:50:31.443262-04:00 syslog04 stunnel: LOG5[509]: Service [rsyslogd] accepted connection from 192.168.1.168:57426 2021-08-30T16:50:31.483560-04:00 syslog04 stunnel: LOG5[509]: s_connect: connected 127.0.0.1:514 2021-08-30T16:50:31.484401-04:00 syslog04 stunnel: LOG5[509]: Service [rsyslogd] connected remote server from 127.0.0.1:54060 2021-08-30T16:50:32-04:00 localhost fs4 fs4[126991]: Connection has been established: from[192.168.1.168] to[syslog04.catl.local] **TLS AD server:** 2021-08-10T12:11:15-04:00 localhost fs4 fs4[115764]: Log: User Directory Login Successful. Details: [192.168.1.168] [ldaps://WINSRV2012R2-01.catl.local:636][tlsv1_2] [forescout@catl.local] Login Successful.. Severity: 6
Termination of the trusted channel	**TLS audit server:** 11/24/2021; 6:39:01 AM; fs4; Socket successfully shutdown. Socket details: Peer ip[syslog04.catl.local], Peer port[6514], type [SSL]; Succeeded. **TLS AD server:** 2021-11-24T06:33:57-05:00 localhost fs4 fs4[114950]: Log: User Directory Disconnect Successful. Details: [192.168.1.168] [ldaps://WINSRV2012R2-01.catl.local:636][forescout@catl.local] Disconnect Successful.. Severity: 6
Failure of the trusted channel functions.	**TLS audit server:** 11/19/2021; 12:06:41 PM; fs4; Socket can't be created. Error: syslog04.catl.local:/unsupported certificate purpose(26) SSL connect attempt failed error:14090086:SSLroutines:ssl3_get_server_certificate:certificate verify failed. Socket details: Peer ip[syslog04.catl.local],Peer port[6514]; Failed. **TLS AD server:** 2021-11-02T14:34:28-04:00 localhost fs4 fs4[2877]: Log: User Directory Connect Error. Details: [192.168.1.168] [ldaps://WINSRV2012R2-01.catl.local:636][negotiate] Connect Failed [WINSRV2012R2-01.catl.local:/unsupported certificate purpose(26) SSL connect attempt failed error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed]. Severity: 3
Initiation of the trusted path	**TLS with AD:** 2021-08-10T12:11:14-04:00 localhost fs4 fs4[115764]: Log: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Details: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Severity: 6

	2021-08-10T12:11:15-04:00 localhost fs4 fs4[115764]: Log: User Directory Login Successful. Details: [192.168.1.168] [ldaps://WINSRV2012R2-01.catl.local:636][tlsv1_2] [forescout@catl.local] Login Successful.. Severity: 6 2021-08-10T12:11:15-04:00 localhost fs4 fs4[115764]: Log: User Directory Disconnect Successful. Details: [192.168.1.168] [ldaps://WINSRV2012R2-01.catl.local:636][forescout@catl.local] Disconnect Successful.. Severity: 6 2021-08-10T12:11:15-04:00 localhost fs4 fs4[115764]: Log: Login success by forescout@192.168.1.99. Details: User forescout logged in from 192.168.1.99. Severity: 6 2021-08-10T12:11:15-04:00 localhost fs4 fs4[115764]: User forescout session 0 changed Enterprise Manager Console. Details: User 'forescout' at host IP 192.168.1.99 attempted to log in to Enterprise Manager 192.168.1.168: Login succeeded<EOL> 5 successful login(s) in the last 60 days. **TLS no AD:** 2021-08-30T17:55:14-04:00 localhost fs4 fs4[130830]: Log: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Details: Loaded ConfigParams: FSAllowedConsoleAddressesParams. Severity: 6 2021-08-30T17:55:14-04:00 localhost fs4 fs4[130830]: Log: Login success by admin@192.168.1.99. Details: User admin logged in from 192.168.1.99. Severity: 6 2021-08-30T17:55:14-04:00 localhost fs4 fs4[130830]: User admin session 0 changed Enterprise Manager Console. Details: User 'admin' at host IP 192.168.1.99 attempted to log in to Enterprise Manager 192.168.1.168: Login succeeded<EOL> 54 successful login(s) in the last 60 days. **SSH:** 2021-08-10T13:20:40-04:00 localhost fs4 sshd[5242]: Connection from 192.168.1.99 port 60747 on 192.168.1.168 port 22 2021-08-10T13:20:47-04:00 localhost fs4 sudo: _fsservice : TTY=unknown ; PWD=/usr/local/forescout ; USER=root ; COMMAND=/bin/fstool netflowtool netflow_init_softflow 2021-08-10T13:20:51-04:00 localhost fs4 sshd[5242]: Accepted password for cliadmin from 192.168.1.99 port 60747 ssh2 2021-08-10T13:20:51-04:00 localhost fs4 fs4[115764]: User cliadmin session 0 changed Authentication. Details: 192.168.1.99 port 60747 ssh2

Termination of the trusted path	**TLS** 2021-08-10T12:18:13-04:00 localhost fs4 fs4[115764]: Log: Logout by forescout@192.168.1.99. Details: User forescout@192.168.1.99 logged out. Severity: 6 2021-08-10T12:18:13-04:00 localhost fs4 fs4[115764]: User forescout session 8218628559389414453 changed Enterprise Manager Console. Details: Logout from 192.168.1.168 by host 192.168.1.99 : Logout succeeded **SSH** 2021-08-10T13:50:05-04:00 localhost fs4 sshd[5321]: Received disconnect from 192.168.1.99 port 60747:11: FlowSshClientSession: disconnected on user's request 2021-08-10T13:50:05-04:00 localhost fs4 sshd[5321]: Disconnected from 192.168.1.99 port 60747
Failure of the trusted path functions	2021-08-16T12:10:05-04:00 localhost fs4 fs4[88707]: Log: Failed to negotiate SSL cipher suite for connection from 192.168.1.98, host name 192.168.1.98. Details: Failed to negotiate SSL cipher suite for connection from 192.168.1.98, host name 192.168.1.98. Severity: 3

Table 8: Forescout Auditable Events

8.1 Audit Storage

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 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 an audit 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 enforces a maximum size of 50MB for the OS log file and 5 OS log files (5 = 1 current plus 4 historical) saved at the OS level.

When the OS log file reaches the maximum size, the log file is closed and renamed sequentially (i.e. audit.log.1, audit.log.2). Therefore, with 5 audit logs and a maximum file size of 50MB each, this 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.

9 Operational Modes

When the TOE is first installed, it is considered to be in its normal operational mode. After initial installation, the TOE must still be placed into its evaluated configuration by performing the steps described in Section 6 of this document. Once placed in the evaluated configuration, the TOE's normal operational mode will perform the functions as described in [3].

There is no separate error mode or other degraded mode of operation. In the event that a POST fails, the TOE will need to be rebooted. If the TOE has been corrupted or the hardware has failed such that rebooting will not resolve the issue, a Security Administrator will need to contact Forescout support per the guidance in Section 10.

10 Additional Support

Forescout provides technical support for its products if needed. Customers can register for a support account at https://www.forescout.com/support/get-support/. Additionally, customers can contact Forescout support by calling 1-866-377-8773 (US) or +1-708-237-6591 (international), or by emailing support@forescout.com.