ForeScout CounterACT
Supplemental Administrative Guidance for Common Criteria
Version 1.0
February 16, 2018

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

1 Introduction .............................................................................................................................................. 3
2 Intended Audience .................................................................................................................................. 3
3 Terminology ............................................................................................................................................ 3
4 References ............................................................................................................................................... 4
5 Evaluated Configuration of the TOE ...................................................................................................... 4
  5.1 TOE Components ................................................................................................................................ 4
  5.2 Supporting Environmental Components .......................................................................................... 5
  5.3 Assumptions ......................................................................................................................................... 6
6 Secure Acceptance, Installation, and Configuration ............................................................................... 7
  6.1 Power-On Self Tests .......................................................................................................................... 8
  6.2 Set up SSH .......................................................................................................................................... 9
  6.3 Certificate Management .................................................................................................................... 10
  6.4 Set up Syslog ...................................................................................................................................... 11
  6.5 Set up Active Directory Server ........................................................................................................ 12
  6.6 Cryptographic Configuration Notice ................................................................................................. 13
7 Secure Management of the TOE ........................................................................................................... 13
  7.1 Authenticating to the TOE ................................................................................................................. 14
  7.2 User Accounts and User Management ............................................................................................ 14
  7.3 Password Management ..................................................................................................................... 15
  7.4 Login Banner ..................................................................................................................................... 15
  7.5 Session Termination ............................................................................................................................ 15
    7.5.1 Admin Logout ............................................................................................................................... 15
    7.5.2 Termination from Inactivity ........................................................................................................ 15
  7.6 System Time Configuration ................................................................................................................. 16
  7.7 Secure Updates ................................................................................................................................... 16
8 Auditing ................................................................................................................................................... 17
  8.1 Audit Storage ...................................................................................................................................... 23
9 Operational Modes .................................................................................................................................. 24
10 Additional Support .................................................................................................................................. 24
## Table of Tables

Table 1 – Evaluated Models .................................................................................................................. 5
Table 2 - Evaluated Components of the Operational Environment ...................................................... 6
Table 3 - Self-Test List with Failure Results .......................................................................................... 9
Table 5 - CounterACT Auditable Events .............................................................................................. 23
1 Introduction

The ForeScout CounterACT (CounterACT) is a hardware appliance whose primary functionality is related to the handling of network traffic. The Collaborative Protection Profile for Network Devices, version 1.0 (NDcPP) defines a network device as “a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network.” Additionally, the NDcPP says that example devices that fit this definition include routers, firewalls, intrusion detection systems, audit servers, and switches that have Layer 3 functionality.

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 CounterACT. 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 also expected to be familiar with the general operation of the CounterACT 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 CounterACT 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 CounterACT 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 CounterACT 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. These terms are also described in the ForeScout CounterACT Security Target.

**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 CounterACT 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] CounterACT® Installation Guide Version 7.0.0

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


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, environmental components that support the security behavior of the TOE, or non-interfering environmental components that were present during testing but are not associated with any security claims:

5.1 TOE Components

The TOE is CounterACT, running the CounterACT software version 7.0. CounterACT is a rack-mounted hardware device. The evaluated models’ specific hardware and configuration is as follows:

<table>
<thead>
<tr>
<th>System Name</th>
<th>Equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ForeScout CounterACT : Appliance (CT-) &amp; Enterprise Manager (CEM-)</td>
<td>ForeScout CounterACT v7.0 operating on CentOS 6.6</td>
</tr>
<tr>
<td>CT-Remote</td>
<td>CT-Remote</td>
</tr>
<tr>
<td>CT-100</td>
<td>CT-100; CEM-05, and CEM-10</td>
</tr>
<tr>
<td>CT-1000; CEM-05, and CEM-10</td>
<td>CT-1000; CEM-05, and CEM-10</td>
</tr>
</tbody>
</table>
### Supporting Environmental Components

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Workstation</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>- Non-dedicated machine:</td>
</tr>
<tr>
<td></td>
<td>- Pentium 3, 1GHz</td>
</tr>
<tr>
<td></td>
<td>- 2GB memory</td>
</tr>
<tr>
<td></td>
<td>- 1GB disk space</td>
</tr>
<tr>
<td></td>
<td>- OS running:</td>
</tr>
<tr>
<td></td>
<td>- Windows 7/8/8.1/10</td>
</tr>
<tr>
<td></td>
<td>- Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>- Linux</td>
</tr>
<tr>
<td></td>
<td>- SSHv2 client installed to access the TOE’s CLI</td>
</tr>
<tr>
<td></td>
<td>- ForeScout CounterACT Console application (Console) installed</td>
</tr>
<tr>
<td>TCP communications</td>
<td>from the Management Workstation to the TOE is secured using:</td>
</tr>
<tr>
<td></td>
<td>- SSH for remote access to the CLI (remote console)</td>
</tr>
<tr>
<td></td>
<td>- TLS for remote access from the Console</td>
</tr>
<tr>
<td></td>
<td>The TOE acts as a server for both protocols.</td>
</tr>
</tbody>
</table>
The TOE’s CLI can also be accessed locally with a physical connection to the TOE using the keyboard/video or the serial port and must use a terminal emulator that is compatible with serial communications (local console).

**Update Server**
A general-purpose computer controlled by the vendor that includes a web server and is used to store software update packages that can be retrieved by product customers using HTTPS/TLS enabled browser or Console. The host of the CounterACT Console provides the secure channel and not the TOE. Therefore, HTTPS is not declared in this ST. The CounterACT device does not automatically download or update itself nor does it connect to the update server directly.

**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.

**Active Directory Server**
A system that is capable of receiving authentication requests using LDAP over TLS and validating these requests against identity and credential data that is defined in an LDAP directory. The TOE is the TLS client for this communication.

**Syslog Server**
The TOE connects to a Syslog Server to send Syslog messages for remote storage via TLS connection where the TOE is the TLS client. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.

**Network Infrastructure**
The network infrastructure contains components such as routers, switches, DNS server, etc.

<table>
<thead>
<tr>
<th>Table 2 - Evaluated Components of the Operational Environment</th>
</tr>
</thead>
</table>

## 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:

- **No general purpose computing capabilities:** The CounterACT product must only be used for its intended purpose. General purpose computing applications, especially those with network-visible interfaces, may compromise the security of the product if introduced.

- **Physical security:** The CounterACT 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.

- **Trusted administration:** The CounterACT 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.
• **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 CounterACT 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).

• **Regular updates:** ForeScout provides regular product updates for the CounterACT 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:** CounterACT protects the administrator’s credentials stored on CounterACT that are used to access it. Additionally, it is assumed that any administrative credentials maintained by an environmental Active Directory Server are secured in order to mitigate the risk of impersonation.

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/](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 Chapters 1 through 4 of [1]. The following must be considered when following these procedures:

1. In Chapter 1, the steps under the ‘FIPS Compliance’ section must be performed for the device to be in the evaluated configuration and utilize the evaluated cryptographic algorithms.
2. In Chapter 2, the steps under the ‘Creating an Out-of-Band IP Management Interface’ section are to be performed.
3. Depending on if the CounterACT device is being configured as an Appliance or CounterACT Enterprise Manager (CEM), only the procedures in Chapters 3 or 4 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 Chapter 3 for both an Appliance and CEM.
   b. Disable ICMP by following the steps under the ‘Configure ICMP Settings’ section of Chapter 3 for both an Appliance and CEM.
   c. The use of RMM3 or iDRAC functionality was not assessed in the evaluation. Procedures for enabling this functionality in Chapters 3 and 4 are not to be performed to configure the devices into their evaluated configuration.

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. Installation of the Console is performed following the procedures describe Chapter 6 of [1] and 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 CounterACT device being connected to. Once authenticated, continue the procedures in Chapter 6 of [1] under the ‘Installing the Cumulative Update Pack’ and ‘Running the Initial Setup Wizard on the Console’ sections.

Once configuration through the initial setup wizard is complete, it is recommended that an 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 on the Management Workstation
2. Authenticate to the TOE via the Console
3. Check the current version of the TOE software:
   a. Navigate to “Tools” > “Options” > “Plugins”.
   b. Select the plugin to be updated and click “About”.
   c. Notate the version and build number.
4. Install the latest software image:
   a. Navigate to “Tools” > “Options” > “Plugins”.
   b. Click “Install”.
   c. Specify the update file (i.e. 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 requesting to continue with the installation or abort; and in the evaluated configuration the abort selection must be chosen.
         2. The next procedure to be followed is Step 8.
5. Proceed through the dialog boxes of the wizard to install the update.
6. Repeat Step 4 if individual plugin files have been provided for update as well.
7. After an update finishes installing, the TOE will normally reboot.
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.

6.1 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.
2. Execute the following command:
   
   `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:
   
   `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:

<table>
<thead>
<tr>
<th>#</th>
<th>Component</th>
<th>Validation</th>
<th>Fail Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Core OS and packages (including OpenSSH)</td>
<td>Built-in RPM Verification</td>
<td>Hard-fail</td>
</tr>
<tr>
<td>3.</td>
<td><code>fipscheck</code> utility</td>
<td>HMAC verified against fipshmac</td>
<td>Hard-fail</td>
</tr>
<tr>
<td>4.</td>
<td>Crypto: OpenSSL</td>
<td><code>fipscheck</code> (including OpenSSL self-check)</td>
<td>Hard-fail</td>
</tr>
<tr>
<td>5.</td>
<td>OpenSSL rpm package</td>
<td>Built-in RPM Verification</td>
<td>Hard-fail</td>
</tr>
<tr>
<td>7.</td>
<td>Core CounterACT and plugin installation packages</td>
<td>SHA-256 verified against last known or stored</td>
<td>Soft-fail</td>
</tr>
<tr>
<td></td>
<td>and extracted files.</td>
<td>hash.</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>System current state vs system configuration</td>
<td>Running kernel version compared to version</td>
<td>Soft-fail</td>
</tr>
<tr>
<td></td>
<td></td>
<td>defined in grub;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FIPS mode running status compared to</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>configuration in grub.</td>
<td></td>
</tr>
</tbody>
</table>

Table 3 - Self-Test List with Failure Results

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

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

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

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, an administrator will need to contact ForeScout support per the guidance in Section 10.

### 6.2 Set up SSH

The TOE acts as an SSH server for remote console (remote CLI) management. In the evaluated configuration an access control list of IP addresses allowed for remote administration is required. This ACL must be configured using the procedures defined under ‘Updating SSH Access’ in Appendix 1 of the [2] document.

The TOE is configured to support the following algorithms for SSH in the evaluated configuration:
- Encryption algorithms: aes128-cbc and aes256-cbc
- Public key algorithm: ssh-rsa
- MAC algorithms: hmac-sha-1, hmac-sha2-256 and 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.

NOTE: The SSH session key thresholds for time and amount of transmitted data are not configurable in the evaluated configuration. The TOE has been configured to rekey before one hour has elapsed or one gigabyte of data has been transmitted using a key; whichever occurs first. No other configuration is allowed.

6.3 Certificate Management

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 CounterACT Console.
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
   b. **Common Name** – <system hostname>
   c. Organization – <organizational name>
   d. Organizational Unit – <unit name>
   e. Locality – <locality name>
   f. State – <state name>
   g. Country Code – <country code>
   h. **Key Length** – RSA-2048
   i. **Signature Algorithm** – SHA-256
   j. 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 ‘Generating CSRs and Importing Signed Certificates’ section of [2].

Importing Trusted CA Certificates

In order for the TOE to authenticate to the remote Syslog and Active Directory servers, trusted CA certificates must be installed into the TOE’s certificate trust store.

Import the required trusted CA certificates by completing the following procedures:
1. Authenticate to the TOE via the CounterACT Console.
2. Click on “Tools” > “Options”.
3. Click on “Certificates” > “Trusted Certificates”.
4. Click “Add”.
5. Specify the Certificate file.
6. Ensure “Enable trusting this certificate” is checked.
7. Click “Next”.
8. Click “Next” after reviewing the certificate data.
9. Ensure “All subsystems” is selected and then click “Next”.
10. Ensure “All CounterAct devices” is selected and then click “Finish”.
11. Click “Apply”.

For more information on importing trusted CA certificates refer to [3]. The procedures above are the ones used during the evaluation which correspond to the ‘Import and Scope Trusted Certificates’ section of [3].

### 6.4 Set up Syslog

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 a syslog interface for remote transmission of these audit records. In the evaluated configuration, this interface is secured using TLS v1.1 and v1.2 and the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

The Syslog Server will need to support at least one of these TLS protocol versions and one of these ciphersuites for communication between the TOE and Syslog Server to be established.

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

1. Authenticate to the TOE via the Console.
2. Choose “Tools” > “Options” from the toolbar.
3. In the Plugins pane, select Syslog and then Configure.
4. Select Add and enter the relevant information for the following fields:
   a. Specify the remote syslog server hostname
   b. Specify the remote syslog server port
   c. Specify the server protocol as TCP
   d. Ensure “Use TLS” is checked
   e. Specify an identity for the transmitted syslog events
   f. Specify the Facility: local4
   g. Specify the Priority: debug
5. On the Configuration window, select the “Default Action Configuration” tab.
6. Specify the following fields:
   a. Specify the remote syslog server hostname
   b. Specify the remote syslog server port
   c. Specify the server protocol as TCP
Specify an identity for the transmitted syslog events  
e. Specify the Facility: local4  
f. Specify the Priority: debug  

7. Select OK.  
8. On the Events filtering tab, ensure “Include Operating System messages” is checked.

For more information on syslog management refer to [4]. The procedures above are the ones used during the evaluation which correspond to the ‘Configuration’ section of [4]. Once syslog is configured, all audit records are stored locally and automatically transferred to the remote Syslog Server as soon as they are generated.

Since syslog functions in a streaming fashion, a communications outage between the TOE and Syslog 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.

6.5 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 v1.1 and v1.2 and the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

The Active Directory Server will need to support at least one of these TLS protocol versions 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.  
2. Click on “Tools” > “Options”.  
3. Click on “User Directory”.  
4. Click “Add”.  
5. Specify the Name field with a description such as “AD”.  
6. Specify the Type as “Microsoft Active Directory”.  
7. Ensure “Use as directory”, “Use for authentication”, and “Use for Console Login” are checked.  
8. Click “Next”.  
9. Specify the Fully Qualified Domain Name of the Active Directory server in the “Address” field.  
10. Specify the TLS port for secure LDAP (e.g. 636).  
11. Specify the domain, administrator bind account, and password data.  
12. Click “Next”.  
13. Specify the test user data in order to verify that the Active Directory configuration was setup correctly.  
14. Click “Finish”.  
15. Select the newly created User Directory and click “Edit”.  


17. Click “OK”.
18. Click “Apply”.
19. Click “Test” to verify that the configuration was setup correctly.
20. From the CounterACT Options panel, select “Console User Profiles”.
21. Click “Add”.
23. Specify the external AD username in the User Name field.
24. Select the Server Name that was chosen in Step 5 (e.g. AD).
25. Click “Next”.
26. Specify the permissions for that user on the CounterACT device.
27. Click “Next”.
28. Click “Finish”.

For more information on Active Directory Server refer to [5]. The procedures above are the ones used during the evaluation which correspond to the ‘Add Servers’ and ‘Microsoft Active Directory Server Settings’ sections of [5].

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.

6.6 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.

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 these documents in full in order to have in-depth awareness of the security functionality of the CounterACT 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 via the serial port 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.

Connecting to the TOE with SSH requires the SSH client to support:

- Encryption algorithms: aes128-cbc and/or aes256-cbc
- Public key algorithm: ssh-rsa
- MAC algorithms: hmac-sha-1, hmac-sha2-256 and/or hmac-sha2-512
- Key exchange method: diffie-hellman-group14-sha1

SSH public key authentication can be achieved for SSH by a user executing the following steps for their 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 their username and password.
4. Type “authorized_keys”
5. Paste the public key in the file that is opened and save the file.

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 6.5 of this document describes configuring the TOE to connect to the Active Directory Server. For more information regarding accessing the TOE via the Console Application refer to Chapter 2 in the [2] document.

7.2 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 the “cliadmin” user for the CLI interfaces and the Administrator users (default account “admin”) for the Console.

For the CLI interfaces, the “cliadmin” user is the only user in the evaluated configuration and for the Console, any user assigned as an Administrator can be used in the evaluated configuration.

All security management functions for the Console are managed by roles (permissions) being assigned to users. Authorized actions for a particular user are dependent on which set of permissions a user has. The Admin User (default user account) cannot change its name or set of permissions (by default all permissions are assigned to the Admin User) assigned to it. The Admin user can create other Administrator users, and change the permissions of those users. The ‘Managing Users’ chapter in [2] describes the various permissions and managing local and external (e.g. Active Directory) users.
7.3 Password Management

In the evaluated configuration, the TOE supports passwords with a minimum length of 15 and an unlimited maximum length. 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. For the Console, an Administrator user has the ability to set the minimum password to 15 characters by performing the following steps:

1. Authenticate to the TOE via the Console.
2. Navigate to “Tools” > “Options” > “Console User Profiles” > “Password and Login”.
3. Specify the password minimum length value to “15”.

For the CLI the “cliadmin” user has the ability to set the minimum character limit for passwords to 15 characters to gain access through the CLI by performing the following steps:

1. Authenticate to the TOE via the Console.
2. Navigate to “Tools” > “Options” > “Plugins” > “CounterACT Infrastructure Update Pack”.
3. Specify the password minimum length value to “15”.

7.4 Login Banner

There are three possible ways to log in to the TOE: local CLI (local console), remote CLI, and a remote Console. When logging in locally or remotely through the CLI, a pre-authentication banner is displayed. It can be configured by an Administrator user via the Console. When connecting remotely via the Console, a pre-authentication banner is displayed that can also be configured by an Administrator user through the Console. Configuration instructions for the banners are in Chapter 14 ‘Login Notice and Consent Message Before Login’ and in Chapter 15 ‘Configure Session Security Features for Command-Line Interaction’ of [2].

NOTE: The pre-authentication banner for the CLI and the Console are configured separately.

NOTE: The pre-authentication banner for the CLI and the Console are the only allowed services prior to authentication to the TOE.

7.5 Session Termination

7.5.1 Admin 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” > “Exit” button.

7.5.2 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 CLI 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 an Administrator. The following steps can be performed to set the CLI and Console timeouts:

**CLI timeout**

1. Authenticate to the TOE via the Console.
2. Select “Options” from the “Tools” menu and then expand the “Plugins” folder.
3. Select “CounterACT Infrastructure Update Pack”
4. Select the “CLI Options” tab.
5. Ensure “Enable configuration options for command-line Appliance” is checked.
6. Specify the value for the Session timeout in minutes.
7. Click “Apply”.

**Console timeout**

1. Authenticate to the TOE via the Console.
2. Select “Options” from the “Tools” menu and then expand the “Console User Profiles” folder.
3. Select “Password and Login”
4. Select the “Session” tab.
5. Select the “User Inactivity Timeout” option and define the period of time to wait before disconnecting inactive sessions.
6. Click “Apply”.

### 7.6 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. An Administrator user can configure all aspects of the clock using the local or remote CLI. The NTP settings must be configured to look to itself and not for a remote NTP server, before setting the time manually (this equates to disabling the NTP services).

1. Authenticate to the SUT via the CLI.
2. Execute the following command:
   
   ```
   ntp setup 127.0.0.1
   ```

Now set the time manually:

3. Execute the following command to set the date and time:

   ```
   date --set “YYYY-MM-DD HH:MM:SS”
   ```

### 7.7 Secure Updates

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

When an update is available, an 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 its latest version:

1. Place the software image on the Management Workstation
2. Authenticate to the TOE via the Console
3. Check the current version of the TOE software:
   a. Navigate to “Tools” > “Options” > “Plugins”.
   b. Select the plugin to be updated and click “About”.
   c. Notate the version and build number.
4. Install the latest software image:
   a. Navigate to “Tools” > “Options” > “Plugins”.
   b. Click “Install”.
   c. Specify the update file (i.e. 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 requesting to continue with the installation or abort; and in the evaluated configuration the abort selection must be chosen.
         2. The next procedure to be followed is Step 8.
5. Proceed through the dialog boxes of the wizard to install the update.
6. Repeat Step 4 if individual plugin files have been provided for update as well.
7. After an update finishes installing, the TOE will normally reboot.
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.

8 Auditing

In order to be compliant with Common Criteria, the TOE audits the events in the table below. Performing the steps in Sections 6.3 and 6.4 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 Syslog Server.

The following is an example of an audit record that CounterACT produces:
Each audit record contains identifying information required by Common Criteria including the date and time the event occurred (Jun 30 12:45:24), the type of event (authentication failure), the subject identity of the event (user=cliadmin), and the outcome of the event (Permission denied).

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

<table>
<thead>
<tr>
<th>Auditable Event</th>
<th>Sample Audit Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to establish an SSH session</td>
<td>Jun 26 18:41:49 192.168.1.42 sshd[38668]: fatal: no matching mac found: client server hmac-sha1,hmac-sha2-256,hmac-sha2-512</td>
</tr>
<tr>
<td></td>
<td>GUI Console Valid Authentication: Jun 28 12:54:00 192.168.1.42 CounterACT[99566]: Log: Login success by admin@192.168.1.25. Details: User admin logged in from 192.168.1.25. Severity: [log_severity].</td>
</tr>
</tbody>
</table>
### SSH CLI Valid Authentication

- **Jun 28 11:45:00 192.168.1.42 sshd[109491]: FIPS mode initialized**
- **Jun 28 11:45:00 192.168.1.42 sshd[109491]: pam_unix(sshd:auth): authentication failure; loginname= uid=0 euid=0 tty=ssh ruser= rhost=josh.cctl.com user=cliadmin**
- **Jun 28 11:45:04 192.168.1.42 sshd[109491]: Failed password for cliadmin from 192.168.1.25 port 51442 ssh2**
- **Jun 28 11:45:07 192.168.1.42 sshd[109493]: Received disconnect from 192.168.1.25: 13: User request**

### Unsuccessful attempt to validate a certificate


### Modification of behavior of the TSF

- **Jul 13 13:32:35 192.168.1.41 FS1[18331]: User admin changed Password and Login. Details: Display this Notice and Consent Message before login value: Previous Value: This is a US GOVERNMENT information system. Any unauthorized use will result in criminal and/or civil prosecution.; Current Value: WARNING WARNING This is a US GOVERNMENT information system. Any unauthorized use will result in criminal and/or civil prosecution. #012**

### Any attempt to initiate a manual update

- **Feb 8 00:16:04 FS1 FS1[48019]: User admin changed Plugin Management. Details: Installation started for plugin: Syslog**

### All management activities of the TSF

- **Feb 12 11:53:18 FS1 FS1[20146]: User admin changed User Directory Configuration. Details: Edited the following User Directory Server AD : OCSP Softfail: Previous Value: false; Current Value: true**

### Changes to the time

- **Sep 20 12:30:00 192.168.1.41 fs-cli[32806]: System time change from: 'Wed Sep 20 12:20:06 2017 (EDT)' to: 'Wed Sep 20 12:30:00 2017 (EDT)'**

### Initiation of update; result of the update attempt (success or failure)

- **Feb 8 00:16:04 FS1 FS1[48019]: User admin changed Plugin Management. Details: Installation started for plugin: Syslog**
- **Feb 8 00:16:09 FS1 FS1[48019]: User admin changed Plugin Management. Details: Upgrade Succeeded for Plugin: Syslog (Version 3.3.0 build 33,009,093)**
<table>
<thead>
<tr>
<th>Event Description</th>
<th>Date/Time</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure of update</td>
<td>Feb 8 00:22:33 FS1 FS1[32227]:</td>
<td>User admin changed Plugin Installation. Details: Invalid zip file structure</td>
</tr>
<tr>
<td></td>
<td>Feb 8 00:23:22 FS1 FS1[32227]:</td>
<td>User admin changed Plugin Installation. Details: Plugin installation failed.</td>
</tr>
<tr>
<td>The termination of a remote session by the session locking mechanism</td>
<td>Aug 3 11:34:12 192.168.1.41 FS1[3182]:</td>
<td>User admin changed Enterprise Manager Console. Details: Logout due to inactivity.</td>
</tr>
<tr>
<td></td>
<td>Aug 3 11:34:18 192.168.1.41 FS1[3182]:</td>
<td>Log: Logout by admin@192.168.1.25. Details: User admin@192.168.1.25 logged out. Severity: {log_severity}</td>
</tr>
<tr>
<td>The termination of an interactive session</td>
<td>Local CLI Session</td>
<td>Jul 13 16:01:34 192.168.1.42 login: pam_unix(login:session): session closed for user cliadmin</td>
</tr>
<tr>
<td></td>
<td>Jul 13 16:01:34 192.168.1.42 init:</td>
<td>serial-ttys0 (/dev/ttyS0) main process ended, respawning</td>
</tr>
<tr>
<td></td>
<td>SSH CLI Session</td>
<td>Jun 23 13:42:28 192.168.1.42 sshd[85903]: Received disconnect from 192.168.1.25: 11: FlowSshClientSession: disconnected on user's request</td>
</tr>
<tr>
<td></td>
<td>GUI Console Session</td>
<td>Jun 23 13:45:30 192.168.1.42 CounterACT[99566]: Log: Logout by admin@192.168.1.25. Details: User admin@192.168.1.25 logged out. Severity: {log_severity}</td>
</tr>
<tr>
<td>Event Type</td>
<td>Date/Time</td>
<td>Details</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Initiation of the trusted path</td>
<td>Jun 26 12:10:30 192.168.1.42</td>
<td>SSH CLI Initiation</td>
</tr>
<tr>
<td></td>
<td>Jun 26 12:10:30 192.168.1.42</td>
<td>Accepted password for cliadmin from 192.168.1.25 port 56969 ssh2</td>
</tr>
<tr>
<td></td>
<td>Jun 26 12:10:30 192.168.1.42</td>
<td>CounterACT[99566]: User 192.168.1.25 changed Authentication. Details: Accepted password for cliadmin from 192.168.1.25 port 56969 ssh2</td>
</tr>
<tr>
<td></td>
<td>Jun 26 12:10:30 192.168.1.42</td>
<td>sshd[56889]: pam_unix(sshd:session): session opened for user cliadmin by (uid=0)</td>
</tr>
<tr>
<td></td>
<td>Jun 26 12:10:32 192.168.1.42</td>
<td>subsystem request for sftp</td>
</tr>
<tr>
<td></td>
<td>Jun 26 12:10:32 192.168.1.42</td>
<td>sudo: cliadmin ; TTY=unknown ; PWD=/ ; USER=root ; COMMAND=/usr/bin/sshd -c /usr/libexec/openssh/sftp-server</td>
</tr>
<tr>
<td>Termination of the trusted path</td>
<td>Jun 26 12:10:38 192.168.1.42</td>
<td>SSH CLI Termination</td>
</tr>
<tr>
<td></td>
<td>Jun 26 12:10:38 192.168.1.42</td>
<td>Updated connection from 192.168.1.25: 11: FlowSSHClientSession: disconnected on user's request</td>
</tr>
<tr>
<td></td>
<td>Jun 26 12:10:38 192.168.1.42</td>
<td>sshd[56893]: pam_unix(sshd:session): session closed for user cliadmin</td>
</tr>
<tr>
<td>Administrative login and logout</td>
<td></td>
<td>See “All uses of the authentication mechanism”</td>
</tr>
<tr>
<td>Security related configuration</td>
<td>Feb 8 07:53:29 FS4 FS4[7221]</td>
<td>Fs: User admin changed CounterACT Infrastructure Update Pack Configuration. Details: Edited the following CounterACT Appliance: : Session timeout (minutes): Previous Value: 80; Current Value: 90</td>
</tr>
<tr>
<td>Generating/import of, changing, or</td>
<td>Feb 7 09:08:07 FS3 FS3[17471]</td>
<td>Fs: User admin changed Configuration. Details: Change trusted certificates configuration definition to Added Fingerprint 'c4650e925d33d4895f3bd163884886a9d9d116', Issued To</td>
</tr>
<tr>
<td>deleting of cryptographic keys</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

21 | Page
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| Resetting passwords | **GUI Password Change**  
Details: User 'user1' changed their password  
**CLI Password Change**  
Jun 27 16:37:20 192.168.1.42: password changed for cliadmin |
| Starting and stopping services (if applicable) | Feb 12 15:58:03: User admin changed Plugin Management.  
Details: User Directory plugin version 6.1.1 build 61,010,081 was Started on Enterprise Manager  
Details: User Directory plugin version 6.1.1 build 61,010,081 was Started on Enterprise Manager |
| Start-up and shut-down of the audit functions | **Start-up and shut-down of the TOE audit functions is synonymous with the powering-off and powering-on of the TOE:**  
Feb 13 10:54:33: rsyslogd: (re)start  
Feb 13 10:54:33: dbserver: redirecting log output to logging collector process#012  
Feb 13 10:54:33: dbserver: Future log output will appear in directory "pg_log". |
| Failure to establish an SSH session | Jun 26 18:41:49: fatal: no matching mac found: client_server hmac-sha1,hmac-sha2-256,hmac-sha2-512 |
| Failure to establish a TLS session | **TLS Client**  
Details: [192.168.1.41] [ldaps://genericopenssl.cctl.com:636] [negotiate] Connect Failed  
#0120:Socket::SSL: SSL connect attempt failed because of handshake problems error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert handshake failure.  
Severity: {log_severity}  
**TLS Server**  
Details: Failed to negotiate SSL cipher suite for connection from 192.168.1.247, host name 192.168.1.247.  
Severity: {log_severity} |
| All uses of the authentication mechanism | **Local CLI Valid Authentication**  
Jun 30 12:45:50: session opened for user cliadmin by LOGIN(uid=0)  
Jun 30 12:45:50: LOGIN ON tty1 BY cliadmin  
Jun 30 12:45:50: sudo: cliadmin : TTY=tty1 ; PWD=/ ; USER=root ; COMMAND=/usr/bin/fstool cli  
Jun 30 12:46:05: login: pam_unix(login:session): session closed for user cliadmin  
**Local CLI Invalid Authentication**  
Jun 30 12:45:24: authentication failure; logname=LOGIN uids=0 euids=0 tty=tty1 ruser= rhost= user=cliadmin  
Jun 30 12:45:27: FAILED LOGIN SESSION FROM (null) FOR cliadmin, Permission denied  
**GUI Console Valid Authentication**  
Jun 28 12:54:00: Login success by admin@[192.168.1.25].  
Details: User admin logged in from 192.168.1.25.  
Severity: {log_severity} |
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 non-configurable threshold is used to trigger the DB purge function. The DB purge function is initiated when 80% of this predefined and non-configurable threshold is exceeded. When the DB threshold is exceeded, the DB purge function deletes entries in a FIFO (oldest events deleted first) fashion. The DB purge function causes a syslog event to be sent by the TOE.

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

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

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

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

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 [6].

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, an 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.