FireEye, Inc.
Common Criteria Guidance Addendum

Prepared By:
Acumen Security
18504 Office Park Dr
Montgomery Village, MD 20886

www.acumensecurity.net
Table Of Contents

1  Overview........................................................................................................................................5
1.1  Supported Platforms..................................................................................................................5
1.2  TOE Delivery..............................................................................................................................5
2  Enabling CC-NDCPP Compliance ..................................................................................................6
2.1  Enabling CC-NDPP Compliance Using the Web UI ................................................................6
2.2  Enabling CC-NDPP Compliance Using the CLI .......................................................................6
2.3  Enabling the Trusted Platform Module .....................................................................................6
3  Using an Audit Server........................................................................................................................8
3.1  Audit Server Requirements.........................................................................................................8
3.2  System Behavior..........................................................................................................................8
3.3  Audit Server Configuration ........................................................................................................8
3.4  Auditable Events ............................................................................................................................9
  3.4.1  Format..................................................................................................................................9
  3.4.2  CC-NDCPP Events ..............................................................................................................9
4  Authentication ..................................................................................................................................13
4.1  Using an Authentication Server (LDAP) ....................................................................................13
4.2  Troubleshooting an LDAP Connection .......................................................................................13
4.3  Authentication Failure Handling ...............................................................................................14
4.4  Password Management ..............................................................................................................14
4.5  Configuring SSH Keys ................................................................................................................14
4.6  Configuring X.509 Certificates .....................................................................................................15
  4.6.1  Reference Identifiers.............................................................................................................15
5  Cryptographic Protocols....................................................................................................................15
  5.1  SSH .......................................................................................................................................15
  5.2  TLS .......................................................................................................................................15
6  Zeroization .....................................................................................................................................16
7  Self-Test ..........................................................................................................................................16
  7.1  Cryptographic POST ..............................................................................................................16
  7.2  Software Integrity .....................................................................................................................16
8  Software Updates ............................................................................................................................17
9  Setting Time .....................................................................................................................................17
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Automatic Logout due to Inactivity</td>
<td>18</td>
</tr>
<tr>
<td>11</td>
<td>Login Banners</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>11.1 Customizing Login Banners and Messages Using the Web UI</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>11.2 Customizing Login Banners and Messages Using the CLI</td>
<td>19</td>
</tr>
</tbody>
</table>
# Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Draft</td>
</tr>
<tr>
<td>1.1</td>
<td>Updated based on feedback</td>
</tr>
</tbody>
</table>
1 Overview

This document is a guide to the FireEye EX Series Appliance implementation of the Common Criteria Network Device Protection Profile v1.0 (CC-NDPP).

1.1 Supported Platforms

Table 1 Supported Platforms

<table>
<thead>
<tr>
<th>Category</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Versions</td>
<td>EX Series Appliances: EX 3500, EX 5500, EX 8500</td>
</tr>
<tr>
<td>Software Version</td>
<td>EX Series Appliances: 8.0</td>
</tr>
</tbody>
</table>

1.2 TOE Delivery

The TOE is delivered via commercial carrier (either FedEx or UPS). The TOE will contain a packing slip with the serial numbers of all shipped devices. The receiver must verify that the hardware serial numbers match the serial numbers listed in the packing slip.


2 Enabling CC-NDCPP Compliance

You can use either the Web UI or the command-line interface to enable CC-NDPP compliance, which performs the following:

- Configures the certified cryptographic components;
- Sets minimum password length
- Enabled certificate validation

Note: After compliance has been enabled on an appliance per the below instructions, you must use SSH from a server or desktop that has the proper ciphers. For example:

```bash
ssh -c aes128-cbc admin@xxx.xxx.xxx.xxx
```

Otherwise, you will get an error message. For example:

```
matching cipher is not supported: des-cbc@openssh.com
```

2.1 Enabling CC-NDCPP Compliance Using the Web UI

To enable CC-NDCPP compliance using the Web UI:

1. On the Web UI, select the Settings tab.
2. Select Compliance on the sidebar.
3. Click Enable FIPS + CC Compliance.
4. Click Reboot Now.
5. Check that there are tick icons in the FIPS column and CC-NDPP columns on the Settings: Compliance page.

2.2 Enabling CC-NDCPP Compliance Using the CLI

To enable CC-NDCPP compliance using the CLI:

1. Enable the CLI configuration mode:
   ```
   hostname > enable
   hostname # configure terminal
   ```
2. Bring the system into CC-NDPP compliance:
   ```
   hostname (config) # compliance apply standard all
   ```
3. Save your changes:
   ```
   hostname (config) # write memory
   ```
4. Restart the appliance:
   ```
   hostname (config) # reload
   ```
5. Verify that the appliance is compliant:
   ```
   hostname (config) # show compliance standard all
   ```

2.3 Enabling the Trusted Platform Module

Use the following procedure to enable the trusted platform module (TPM) for CC-NDPP configurations.
**Note:** You enable the TPM only once. You cannot undo this procedure.

**Prerequisites**

- Administrator access
- TPM is present.
- Keyboard directly attached to the appliance
- No serial console or IPMI console attached to the appliance

To enable the TPM:

1. Enter the CLI configuration mode:
   ```
   hostname > enable
   hostname # configure terminal
   ```

2. Check if the TPM is present and enabled.
   ```
   hostname (config) # show tpm
   ```
   In the following example, there is a TPM, but it is disabled:
   ```
   Trusted Platform Module:
   Present: yes
   Enabled: no
   Physical Presence Interface:
   Request Pending: No request pending
   Request Response: 0: No Recent Request
   ```

3. Enable the TPM:
   ```
   hostname (config) # tpm enable
   ```

4. After reading the warning, select yes to continue.

5. Restart the appliance.

If you enable the TPM but do not have a keyboard directly attached to your appliance, you might lose access to the system after it restarts.

6. The system stops at the BIOS POST screen. Press F10 on a directly attached keyboard.

7. Check that the TPM is enabled. For example:
   ```
   hostname (config) # show tpm
   ```
   ```
   Trusted Platform Module:
   Present: yes
   Enabled: yes
   ```
3 Using an Audit Server

Use the following procedure to configure an audit server.

3.1 Audit Server Requirements

The audit server must be a Syslog server that supports TCP and TLS 1.1 or TLS 1.2.

3.2 System Behavior

When configured to use an audit server the EX appliance transmits audit events to the audit server at the same time logs are written locally to non-volatile storage. If the connection fails, the EX continues to store audit records locally and will transmit any stored contents when connectivity to the syslog server is restored.

The amount of audit data that can be stored locally is configurable by setting the local log rotation parameters – refer to the logging files rotation command in the CLI Reference. When the local log is full, the oldest log files are deleted to allow a new log to be created.

3.3 Audit Server Configuration

To use an audit server:

1. Enter the CLI configuration mode:
   hostname > enable
   hostname # configure terminal

2. Specify the protocol to log in to the remote host. For example:
   hostname (config) # logging rsyslog-server protocol tcp
   where rsyslog-server is the hostname or IP address of a rsyslog server where you want to send auditing messages.

   The previous command includes the following parameters:
   ip_address: IP address or hostname of a syslog server where you want to send log messages (rsyslog-server in the example).
   Protocol: Protocol to use for transferring syslog records. For NDcPP compliance, logs must be transferred via TCP.

3. Enable remote logging with encryption:
   hostname (config) # logging rsyslog-server encryption enable
   Encryption is required for compliance with CC.

   The previous command includes the following parameters:
   Encryption: Enable turns on TLS cryptography for audit records.

4. Save your changes:
   hostname (config) # write memory

5. Check the status:
   hostname (config) # show logging
For example, a typical configuration for compliance purposes would capture only auditing messages at the notice level and above.

EX-8500-160 (config) # logging 172.16.225.63 protocol tcp
EX-8500-160 (config) # logging 172.16.225.63 encryption enable
EX-8500-160 (config) # write memory
Saving configuration file ... Done!
EX-8500-160 (config) # show logging
Local logging level: info
Override for class mgmt-back: notice
Override for class mgmt-front: notice
Remote syslog default level: notice
Remote syslog servers:
172.16.225.63 notice
protocol: tcp
encryption: yes

3.4 Auditable Events

3.4.1 Format

The following is the general format of all syslog messages (unless otherwise specified):

Timestamp Hostname process name[pid]: [subsystem.priority]: Message content

For example, a locally logged message looks like this:

May 7 18:27:40 EX-8500-160 pm[5916]: [pm.NOTICE]: AUDIT: System initialization completed

For example, a remotely logged message (excluding any remote post-processing) looks like this:

May 7 18:27:40 EX-8500-160 pm[5916]: [pm.NOTICE]: AUDIT: System initialization completed

Audit events that are related to a user include the related username and other related information such as IP address if available, for example:

May 26 10:01:31 nx-2300-14 mgmtd[4085]: [mgmtd.NOTICE]: AUDIT: User login: username 'admin', full name 'System Administrator', role 'admin', client 'CLI', line 'pts/1', remote address '10.2.6.83', auth method 'local', auth submethod 'password', session ID 251606

3.4.2 CC-NDCPP Events

Table 2 identifies CC-NDCPP relevant audit events.

Table 2 CC-NDCPP Audit Events
<table>
<thead>
<tr>
<th>CC-NDCPP Reference</th>
<th>Auditable Events</th>
<th>EX Audit Event</th>
</tr>
</thead>
</table>
| FAU_GEN.1           | Start-up and shut-down of the audit functions | [mgmtd.NOTICE]: AUDIT: system logger is started  
                      [mgmtd.NOTICE]: AUDIT: shutting down system logger |
|                     | Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators). | Login:  
pam_tallybyname(sshd:account): Successful login for user 'admin'  
Logout:  
mgmtd[4368]: [mgmtd.NOTICE]: AUDIT: User logout: username 'admin', full name 'System Administrator', role 'admin', client 'CLI', line 'pts/1', remote address '192.168.128.124', auth method 'local', auth submethod 'password', session ID 119498 |
<p>|                     | Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed). | 2017-06-07T13:20:38 neon mgmtd[6479]: [mgmtd.INFO]: SET: ** |
|                     | 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). | [mgmtd.NOTICE]: AUDIT: Config change ID 5733: item 1: Certificate name web-cert, ID ea4c414d48b124caf34ec8eeb5504321a7 added |
| FIA_UIA_EXT.1       | All use of the identification and authentication mechanism. | [mgmtd.NOTICE]: AUDIT: User login: username 'username', full name 'full name', role 'admin', client 'session-type', line 'terminal', remote address 'remote-ip', auth method 'method', auth submethod 'submethod', session ID session-id |
| FIA_UAU_EXT.2       |                                                | |
| FMT_MOF.1/ManualUpdate | Any attempt to initiate a manual update | [cli.NOTICE]: AUDIT: user admin: Executing command (image install image-emps_bad_sig.img) |
| FMT_MTD.1/CoreData  | All management activities of TSF data. | 2017-06-07T13:20:38 neon mgmtd[6479]: [mgmtd.INFO]: SET: ** |
| FPT_TUD_EXT.1       | Initiation of update; result of the update attempt (success or failure) | [cli.NOTICE]: AUDIT: user admin: Executing command (image install image-emps_bad_sig.img) |</p>
<table>
<thead>
<tr>
<th>CC-NDCPP Reference</th>
<th>Auditable Events</th>
<th>EX Audit Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPT_STM_EXT.1</td>
<td>Discontinuous changes to time – either Administrator actuated or changed via an automated process.</td>
<td>Timestamp Hostname mgmtd[pid]: [mgmtd.NOTICE]: AUDIT: Action ID ID: requested by: user username (full name) via session Timestamp Hostname mgmtd[pid]: [mgmtd.NOTICE]: AUDIT: Action ID ID: descr: system clock: set date and time Timestamp Hostname mgmtd[pid]: [mgmtd.NOTICE]: AUDIT: Action ID ID: param: date and time: date and time For example: May 27 16:57:08 nx-2300-14 mgmtd[4085]: [mgmtd.NOTICE]: AUDIT: Action ID 2787: requested by: user admin (System Administrator) via CLI (session ID 251576) May 27 16:57:08 nx-2300-14 mgmtd[4085]: [mgmtd.NOTICE]: AUDIT: Action ID 2787: descr: system clock: set date and time May 27 16:57:08 nx-2300-14 mgmtd[4085]: [mgmtd.NOTICE]: AUDIT: Action ID 2787: param: date and time: 1970/01/01 00:00:00 Jan 1 00:00:00 nx-2300-14 mgmtd[4085]: [mgmtd.NOTICE]: AUDIT: Time change detected, clock was moved 16582d 16h 57m 8.301s backward</td>
</tr>
<tr>
<td>FTA_SSL_EXT.1</td>
<td>The termination of a local session by the session locking mechanism.</td>
<td>[cli.NOTICE]: AUDIT: user username: Automatic logout due to keyboard inactivity</td>
</tr>
<tr>
<td>FTA_SSL.3</td>
<td>The termination of a remote session by the session locking mechanism.</td>
<td>[cli.NOTICE]: AUDIT: user username: Automatic logout due to keyboard inactivity</td>
</tr>
<tr>
<td>FTA_SSL.4</td>
<td>The termination of an interactive session.</td>
<td>[wsmd.NOTICE]: AUDIT: Web session 5 timed out due to inactivity [mgmtd.NOTICE]: AUDIT: User logout: username 'admin', full name 'System Administrator', role 'admin', client 'web', line 'web/5', remote address '10.10.131.130', auth method 'local', auth submethod 'password'</td>
</tr>
<tr>
<td>FTP_ITC.1</td>
<td>Initiation of the trusted channel. Termination of the trusted channel.</td>
<td>Audit Server (rsyslog): stunnel_secure_channel: Connected to remote-ip:remote-port using cipher suite cipher Authentication Server (LDAP): ldap_secure_channel: STARTTLS connection</td>
</tr>
<tr>
<td>CC-NDCPP Reference</td>
<td>Auditable Events</td>
<td>EX Audit Event</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>FTP_TRP.1/SSH</td>
<td>Initiation of the trusted path.</td>
<td>SSH2 connection is established with remote-ip port remote-port [preauth] sshd secure channel: sshd is terminated</td>
</tr>
<tr>
<td></td>
<td>Termination of the trusted path.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failure of the trusted path functions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSH Failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sshd[15945]: AUDIT: Authentication failure for user 'admin' from host: 10.10.128.11 tty: unknown</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sshd[30583]: ssh secure channel: atomicio failed: Broken pipe</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TLS / HTTPS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Timestamp hostname httpd: httpd secure channel: SSL connection is established with remote-ip using cipher suite cipher.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>httpd secure channel: connection closed to remote-ip with standard shutdown (server server-hostname:server-port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TLS/HTTPS Failure</td>
</tr>
<tr>
<td>FMT_MTD.1/CryptoKeys</td>
<td>Management of cryptographic keys.</td>
<td>[mgmtd.NOTICE]: AUDIT: Config change ID 5733: item 1: Certificate name web-cert, ID ea4c414d48b124caf34ecca04ec8eeb5504321a7 added</td>
</tr>
<tr>
<td>FCS_HTTPS_EXT.1</td>
<td>Failure to establish a HTTPS session</td>
<td>httpd: httpd secure channel: SSL library error 1 in handshake with 10.10.128.154 (server localhost:443)</td>
</tr>
<tr>
<td>FCS_SSHS_EXT.1</td>
<td>Failure to establish an SSH session</td>
<td>sshd[15945]: AUDIT: Authentication failure for user 'admin' from host: 10.10.128.11 tty: unknown</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sshd[30583]: ssh secure channel: atomicio failed: Broken pipe</td>
</tr>
<tr>
<td>FCS_TLSC_EXT.1</td>
<td>Failure to establish a TLS Session</td>
<td>LDAP: sshd[11661]: pam_ldap: ldap_starttls_s: server <a href="http://www.fireeye.com:389">www.fireeye.com:389</a>: Connect error</td>
</tr>
<tr>
<td>CC-NDCPP Reference</td>
<td>Auditable Events</td>
<td>EX Audit Event</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sshd[21853]: pam_ldap: ldap_starttls_s: server xyz.com:389: Can't contact LDAP server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rsyslog: FireEye-CM stunnel: stunnel secure channel: Failed to Connect to 192.168.128.124:6515</td>
</tr>
<tr>
<td>FCS_TLSS_EXT.1</td>
<td>Failure to establish a TLS Session</td>
<td>httpd: httpd secure channel: SSL library error 1 in handshake with 10.10.128.154 (server localhost:443)</td>
</tr>
<tr>
<td>FCS_TLSS_EXT.2</td>
<td></td>
<td>sshd[6499]: pam_ldap: ldap_starttls_s: server <a href="http://www.fireeye.com:389">www.fireeye.com:389</a>: Connect error: certificate verify failed (self signed certificate)</td>
</tr>
<tr>
<td>FIA_X509_EXT.1/Rev</td>
<td>Unsuccessful attempt to validate a certificate</td>
<td>sshd[6499]: pam_ldap: ldap_starttls_s: server <a href="http://www.fireeye.com:389">www.fireeye.com:389</a>: Connect error: certificate verify failed (self signed certificate)</td>
</tr>
</tbody>
</table>

### 4 Authentication

#### 4.1 Using an Authentication Server (LDAP)

An LDAP authentication server may be used in CC-NDPP mode.

To be CC-NDPP compliant, the following must be enabled:

1. Enable TLS
   
   ```
   hostname (config) # ldap ssl mode tls
   ```

   The previous command includes the following parameters:

   **ssl**: This enables protected communications with the LDAP server. The mode must be set to TLS.

2. Enable Certificate Validation
   
   ```
   hostname (config) # ldap ssl cert-verify
   ```

   The previous command includes the following parameters:

   **Cert-verify**: This enables certificate validation.

#### 4.2 Troubleshooting an LDAP Connection

The following sample log messages will help you troubleshoot an LDAP connection. If you do see similar log messages to the ones listed, use the `show ldap` command and check the settings for all LDAP-related items.


A log message similar to this one indicates that the LDAP ciphers have failed.
A log message similar to this one indicates that your appliance could not reach the LDAP server.

A log message similar to this one indicates that the certificate failed.

4.3 Authentication Failure Handling

The following settings are relevant for CC-NDPP:

1. Configure the number of failed attempts in accordance with your organization’s policies (this setting is automatically applied to all administration interfaces):
   
   hostname (config) # aaa authentication attempts

2. To unlock an account:
   
   hostname (config) # aaa authentication attempts reset

4.4 Password Management

Passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(”, “)”, “\”, “|”, “_”, “`”, “{”, “|”, “}”, “~”).

The TOE is capable of configuring strong passwords, such as those with at least 15 characters long and the following complexity rules:

- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character

To configure criteria that determines the strength of the passwords created for this appliance or sensor, use the `aaa authentication password` commands in CLI configuration mode. To restore the default settings for any password strength rule, type `no` in the CLI command line, followed by the configuration command.

The appliance maintains a minimum password length of 8 characters by default. The minimum password length can be configured using the following command:

1. `aaa authentication password local length`

The previous command includes the following parameters:

`Local Length`: This sets the minimum password length and has a range of 8 to 32 characters.

4.5 Configuring SSH Keys

Use the commands in this section to create a new public key for SSH user authentication. You can use this key instead of the password to authenticate the remote user.

1. Create the public key:
hostname (config) # cmc auth ssh-rsa2 identity key-name generate

The previous command includes the following parameters:

Key-Type: This is the type of key used. For CC compliance, the key must be ssh-rsa2

Key-Name: This is the user-friendly name of the key

2. Save your changes:
hostname (config) # write memory

4.6 Configuring X.509 Certificates

To issue a certificate signing request (CSR), the following command must be executed,

crypto certificate signing-request generate

The base command above generates a CSR without the optional common name. In order to generate a CSR with a common name, the request must be made with the following option,

Name – This is the common name of the device

After a certificate is generated from an external server, the full path certificate must be uploaded to the TOE using the following command,

crypto certificate name <name of the certificate> public-cert
match csr <name of the CSR>

The full public certificate must then be copied to the command line.

4.6.1 Reference Identifiers

Reference identifiers are drawn from the Common Name of certificates installed on the TOE. Checking of the Reference Identifier/Common Name is enabled by enabling compliance mode.

5 Cryptographic Protocols

Enabling CC-NDCPP compliance will ensure that only certified algorithms and key sizes are available for use by the appliance.

5.1 SSH

No configuration is required other than enabling CC-NDCPP compliance.

If a trusted path using the remote CLI over SSH is unintentionally broken, the SSH client will be required to manually reestablish the connection.

5.2 TLS

No configuration is required other than enabling CC-NDCPP compliance.

If a trusted path using the remote Web UI over TLS is unintentionally broken, the web browser will be required to reestablish the connection. The web browser may choose to attempt this reconnection automatically, or it may prompt the user to retry manually.

The TOE will automatically attempt to re-establish an unintentionally disrupted channel to the remote audit server indefinitely. During this time, audit messages continue to be stored locally on the TOE. Once the disruption has been corrected, the syslog client on the TOE will automatically attempt to re-negotiate the TLS channel upon the next retry.
The TOE will automatically attempt to re-establish an unintentionally disrupted channel to the remote LDAP server according to the configuration of the `ldap timeout` CLI settings. If the LDAP server is unable to determine the user authentication attempt is permitted, then the system will deny access to the authentication attempt.

### 6 Zeroization

Use zeroization to overwrite all passwords, keys, and non-active configuration files with zeros.

**Note:** This action cannot be undone.

To zeroize an appliance:

1. Enable the CLI configuration mode:
   ```
   hostname > enable
   hostname # configure terminal
   ```
2. Overwrite all passwords, keys, and non-active configuration files with zeros:
   ```
   hostname (config) # compliance declassify zeroize
   ```

### 7 Self-Test

#### 7.1 Cryptographic POST

During the cryptographic power-on self-test (POST), the appliance invokes the self-test routine provided by the cryptographic library. This self-test performs various checks, including checks that ensure the integrity of the library stored on disk, the proper operation of the cryptographic algorithms, and the soundness of the random number generators. If the self-test fails, then the appliance is forced to restart.

**Note:** The cryptographic POST is run automatically when the appliance is turned on or restarted, regardless of whether the appliance has been put in FIPS 140-2 or CC-NDPP compliance.

The appliance will not run if the cryptographic POST fails upon every restart. A brief informative message is displayed on the console when the FIPS 140-2 cryptographic POST starts:

```
Running FIPS crypto POST...
```

If the POST is successful, the following message is displayed:

```
Done
```

If the POST fails, the following message appears on the console:

```
FIPS crypto POST failed. Automatic reboot in progress.
```

#### 7.2 Software Integrity

The Software Integrity Test is run automatically on start-up, and whenever the system images are loaded. A hash verification is used to confirm the image file to be loaded has not been corrupted and has maintained its integrity. The appliance will not run if the integrity POST fails upon every restart.

If the POST fails, the following message appears on the console:

```
FIPS crypto POST failed. Automatic reboot in progress.
```

No specific administrative interaction is required if an error is encountered. The reboot process will happen automatically and will TOE will not start unless the tests have passed.
8 Software Updates

To perform a software update, query the currently active version and view installation status (allows the administrator to see the installed but inactive version). Use the following commands to install new software images,

1. Download the software image:
   hostname (config) # fenet image fetch

2. View download progress:
   hostname (config) # show fenet image status

3. Install the downloaded software image:
   hostname (config) # image install image-lms_7.9.0.img
   hostname (config) # image boot next

4. Save changes:
   hostname (config) # write memory

Software image files are digitally signed so their integrity can be automatically verified during the upgrade process. An image that fails an integrity check will not be loaded.

9 Setting Time

For CC-NDCPP compliance, time may be manually set or synchronized with an NTP server. To set the date and time, use the following commands,

1. Use the clock set : command to specify the time and date. For example, the following command sets the time and date to 2:00 p.m. on July 21, 2014:
   hostname (config) # clock set 14:00 2014/07/21

2. Use the clock timezone command to specify the time zone. For example, both of the following commands set the time zone to Pacific Standard Time:
   hostname (config) # clock timezone UTC-offset UTC+8
   hostname (config) # clock timezone America North United_States Pacific

3. To restore the default time zone:
   hostname (config) # no clock timezone

4. View the configured time and date settings:
   hostname (config) # show clock

5. Save changes.
   hostname (config) # write memory

To set up a NTP server, use the following commands,

1. To enable NTP synchronization:
   hostname (config) # ntp enable
2. Use the ntp server command to specify the NTP server. Either IP address or DNS address will suffice. For example, both of the following commands set a NTP server
   hostname (config) # ntp server 10.1.1.10
   hostname (config) # ntp server myntpserv.com

3. To force synchronization with a NTP server, use ntpdate command. For example, the following command synchronizes with IP address NTP server 10.1.1.10
   hostname (config) # ntpdate 10.1.1.10

4. To disable NTP synchronization:
   hostname (config) # ntp disable

5. View the configured time and date settings:
   hostname (config) # show clock

6. Save changes
   hostname (config) # write memory

10 Automatic Logout due to Inactivity

To configure maximum inactivity times for administrative sessions (after which time the user is automatically logged out and the session is terminated):

- **Web UI** – refer to the webui auto-logout command in the CLI Reference.
- **CLI** – refer to the cli session auto-logout command in the CLI Reference.

Setting the CLI session idle timeout will simultaneously affect both the remote CLI and the local CLI interfaces.

11 Login Banners

You can customize or remove the messages that appear when users log in to the TOE. You can configure three messages:

- **Remote Banner** - Shown on the Web UI login page and SSH login page.
- **Local Banner** - Shown after the username is entered in the CLI session.
- **Message of the Day** - Shown after the user is authenticated and logged into the appliance CLI.

11.1 Customizing Login Banners and Messages Using the Web UI

Use the **Login Banner** page to configure the messages users see when they log in to the NX Series appliance
11.2 Customizing Login Banners and Messages Using the CLI

Use the CLI commands in this topic to configure the messages users see when they log in to the appliance.

1. To change the local login message only, use the following command:
   `hostname (config) # banner login-local "<text>"`

2. To change the remote login message only, use the following command:
   `hostname (config) # banner login-remote "<text>"`

3. To change the message of the day, use the following command:
   `hostname (config) # banner motd "<text>"`

4. To clear the local login message, the remote login message, or both:
   `hostname (config) # banner login ""
   hostname (config) # banner login-local ""
   hostname (config) # banner login-remote ""`

5. To clear the message of the day:
   `hostname (config) # banner motd ""

6. To restore the default messages:
   `hostname (config) # no banner login
   hostname (config) # no banner motd`

7. Save changes.
hostname (config) # write memory