FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4 Guidance

Document Version: 1.4

Prepared By:
Acumen Security
2400 Research Blvd, Suite 395
Rockville, MD 20850

www.acumensecurity.net

Table of Contents

Revision History

Version	DATE	Description
1.0	04/30/2023	Initial Release
1.1	06/12/2024	Updated few sections
1.2	07/26/2024	Updated few sections
1.3	08/21/2024	Addressed ECR comments
1.4	10/17/2024	Updated the software version to 10.0.4

1 Overview

This document is a guide to the FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliance v10.0.4 implementation of the Common Criteria Network Device Protection Profile v2.2e (CC-NDPP).

1.1 Supported Platforms

Table 1- Supported Platforms

Category	Identifier
Physical Appliances	AX5600 CM4600 CM7600 CM9600 EX3600 EX5600 EX8600 FX6600 HX4600 NX2600 NX3600 NX4600 NX5600 NX6600 NX8600 VX5600 VX12600
Virtual Appliances	CM1500V CM2500V CM7500V EX5500V FX2500V HX4502V HX4600V NX1500V NX2500V NX2550V NX4500V NX6500V NX7500V NX8500V NX10500V
Software Version	10.0.4

FireEye AX, CM, EX, FX, HX, NX, and VX Series are network devices comprised of hardware and software. The virtual devices as defined in **Table *1*** are considered virtual network devices as defined in Case 1 of NDcPP 2.2e running on general purpose hardware and virtualization system which are outside of the TOE. In the virtual case, the TOE boundary represents the virtual network device only. The hardware appliances are physical devices comprised of the TOE firmware running on bare metal, where the TOE boundary is inclusive of hardware and software. Please see Section 1.3 of ST (FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances running TRFEOS 10.0.4 Security Target) for additional details on the TOE models.

The FireEye Malware Analysis (AX) series is a group of forensic analysis platforms that give security analysts hands-on control over powerful auto-configured test environments to safely execute and inspect advanced malware, zero-day and advanced persistent threat (APT) attacks embedded in Web pages, email attachments and files.

FireEye Central Management (CM) series consolidates the administration, reporting and data sharing of the FireEye products in one easy-to-deploy, network-based solution.

The FireEye Email Security (EX) Series Appliances are network devices that secure against advanced email attacks by using signature-less technology to analyze email attachments and quarantine malicious emails.

The FireEye Threat Prevention (FX) platform protects data assets against attacks originating in a wide range of file types. Web mail, online file transfer tools, the cloud, and portable file storage devices can introduce malware that can then spread to file shares and content repositories.

The FireEye Endpoint Security (HX) Appliances are network devices providing organizations with the ability to continuously monitor endpoints for advanced malware and indicators of compromise.

FireEye Network Security (NX) is an effective cyber threat protection solution that helps organizations minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in Internet traffic.

The FireEye Network Threat Prevention Platform (VX) identifies and blocks zero-day Web exploits, droppers (binaries), and multi-protocol callbacks to help organizations scale their advanced threat defenses across a range of deployments, from the multi-gigabit headquarters down to remote, branch, and mobile offices. FireEye Network with Intrusion Prevention System (IPS) technology further

optimizes spend, substantially reduces false positives, and enables compliance while driving security across known and unknown threats.

Note: Each model of the TOE shares an identical codebase employing all NDcPP required functionality. Breach detection, email analysis, endpoint monitoring, IPS, malware analysis, and threat prevention features are not evaluated as part of the Common Criteria certification and are excluded by the evaluation.

1.2 TOE Delivery

For Physical Device:

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.

For Virtual Device:

Vendor sends a welcome email to customers along with a link to download virtual image (OVA) files (e.g., for NX products, https://cloud.fireeye.com/fenet/channel/stable/va/wmps/ [cloud.fireeye.com]).

To download the virtual model image, customers must enter credentials, which they will be provided using an out-of-band mechanism.

1.3 Assumptions

The following assumptions are drawn directly from the [NDcPP].

Table 2 - Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on

	the platform
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.VS_ISOLATON	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical Platform.
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

1.4 Organizational Security Policies

The following Organizational Security Policies are drawn directly from the [NDcPP]:

Table 3 - OSPs

ID	OSP
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

1.5 Operational Environment

The TOE supports the following hardware, software, and firmware components in its operational environment.

Table 4 - Required non-TOE Hardware/ Software/Firmware

Component	Usage/Purpose Description for TOE performance
Virtual Hardware	Virtual hardware provided by VMware vSphere ESXi 7.0 and Intel Xeon E5-4620 v4 (Broadwell)
Management Workstation with Web browser and SSH Client	This includes any IT Environment Management workstation with an SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used. Any web browser that supports TLS 1.2 may be used.
Audit server	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE. The syslog server must support communications using TLS 1.2.
NTP Server	NTP server supporting SHA-1 integrity verification.

2 Initial Setup of the TOE

The FireEye AX, CM, EX, FX, HX, NX, and VX Series devices must be given basic configuration via console connection prior to being connected to any network.

2.1 Using the Console

To access the CLI of the appliance using the console port, follow these steps:

1. Connect the serial port of your computer directly to the DB-9 console port on the FireEye appliance.
2. Open a terminal program on your system, such as Putty.
3. Configure the serial communication settings of your program as follows:
   - Bits per second: 115,200
   - Data bits: 8
   - Stop bit: 1
   - Parity: None
4. When prompted, enter your username and password.

2.2 Basic Configuration

To assign a hostname to the TOE:

```
fireeye-Appliance(config) #  hostname XXXX
```

To assign an IP address to an interface:

```
fireeye-Appliance(config) # interface ether1 ip address xxx.xxx.xxx.xxx
/24 or
fireeye-Appliance(config) # interface ether1 ip address xxx.xxx.xxx.xxx
255.255.255.0
```

To assign an IPv6 address and to enable the interface:

```
fireeye-Appliance(config) # interface ether1 ipv6 address
xxxx:xxxx:xxxx:xxxx::xxxx/64
fireeye-Appliance(config) # interface ether1 ipv6 enable
```

To verify the IPv4 and IPv6 interface status:

```
fireeye-Appliance(config) # sh interface ether1 brief
```

To assign a default gateway to the device:

```
fireeye-Appliance(config) # ip default-gateway <IP address of default
gateway>
fireeye-Appliance(config) # ip default-gateway xxx.xxx.xxx.xxx
```

To assign a name server:

```
fireeye-Appliance(config) # ip name-server <DNS Server IP address>
fireeye-Appliance(config) # ip name-server xxx.xxx.xxx.xxx
```

To save the configuration:

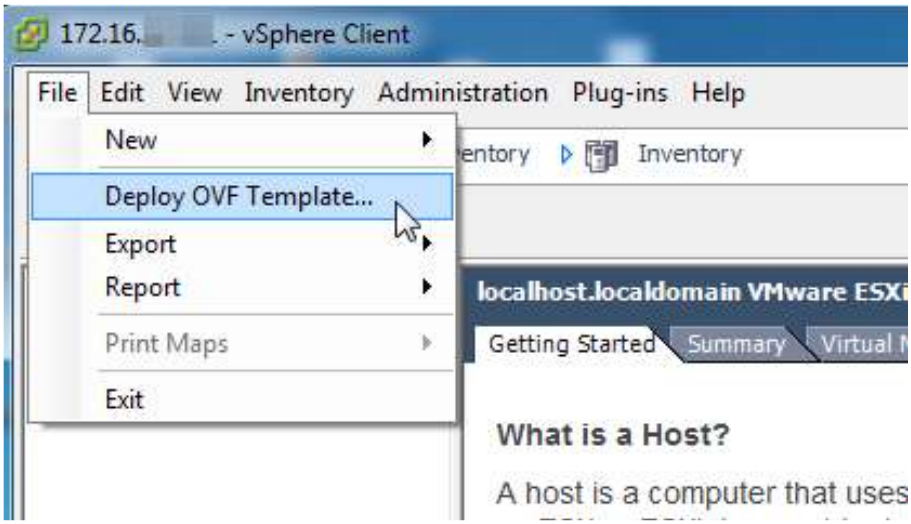
```
fireeye-Appliance(config) # write memory
Saving configuration file ... Done!
```

2.3 For Virtual appliances

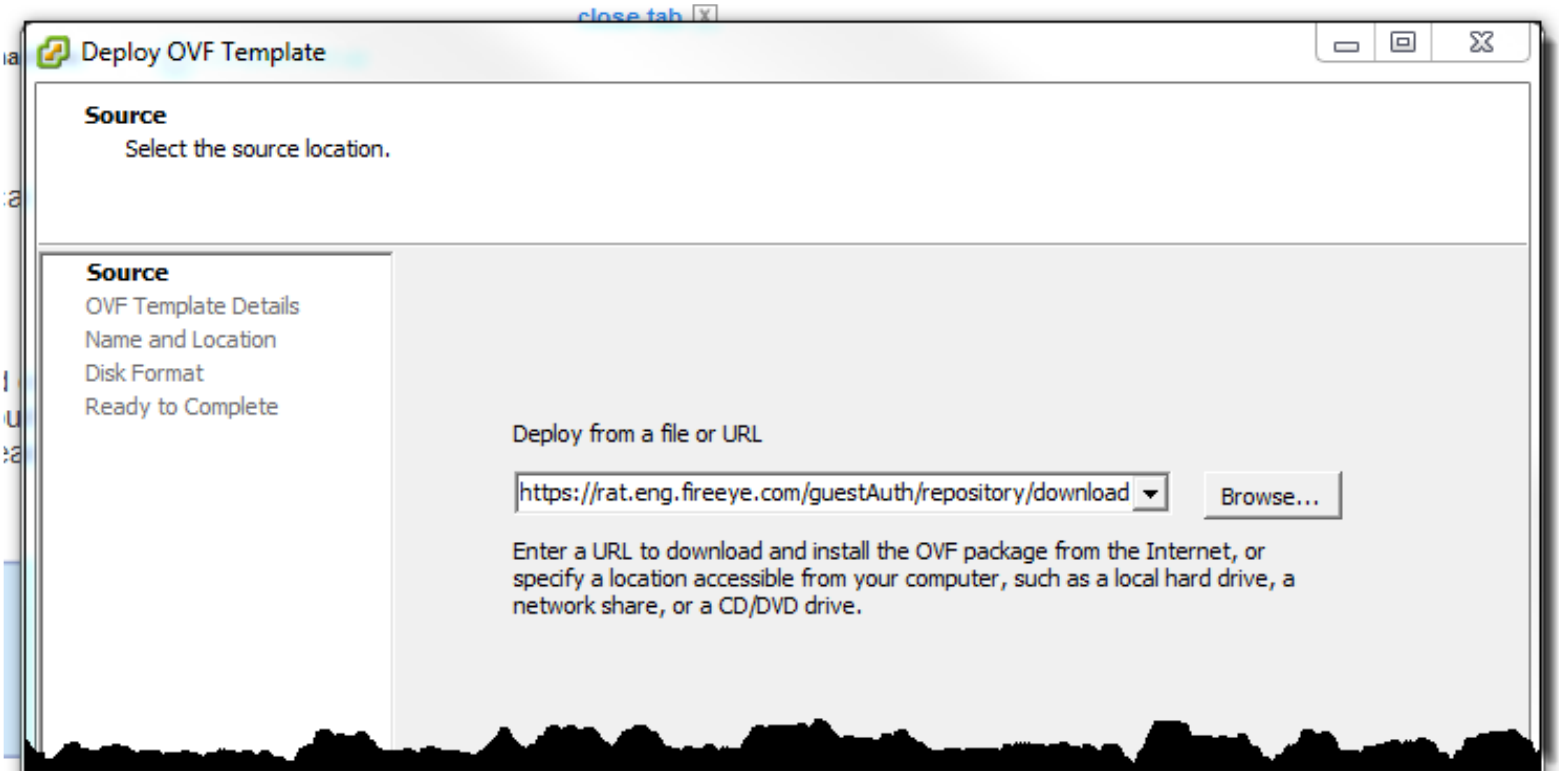
Open Virtualization Format (OVF) is an open standard for various virtualization platforms and is used to package and distribute the software that runs on virtual machines. A virtual appliance is packaged as an OVA image, which is a compressed file containing the contents of an OVF folder. The OVF folder contains the Network Security, Central Management System, or File Protect software image as well as virtual machine files. You install a virtual appliance in a VMware ESXi host.

Appliances on-premises deployment include ESXi, KVM, and Hyper-V.

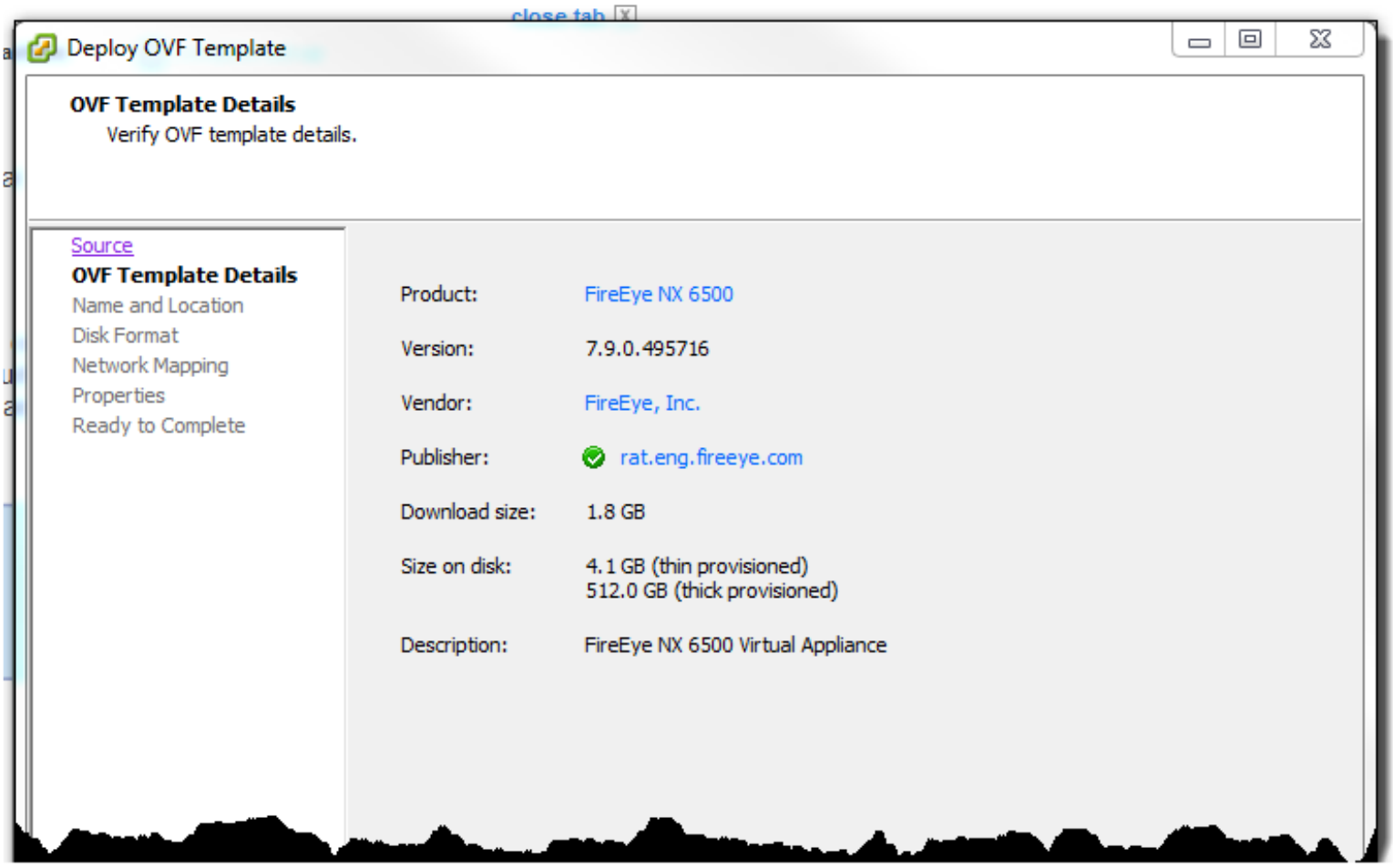
- To install a virtual appliance:
  - Log in to vSphere Client.
  - From the File menu, select Deploy OVF Template to start the wizard.



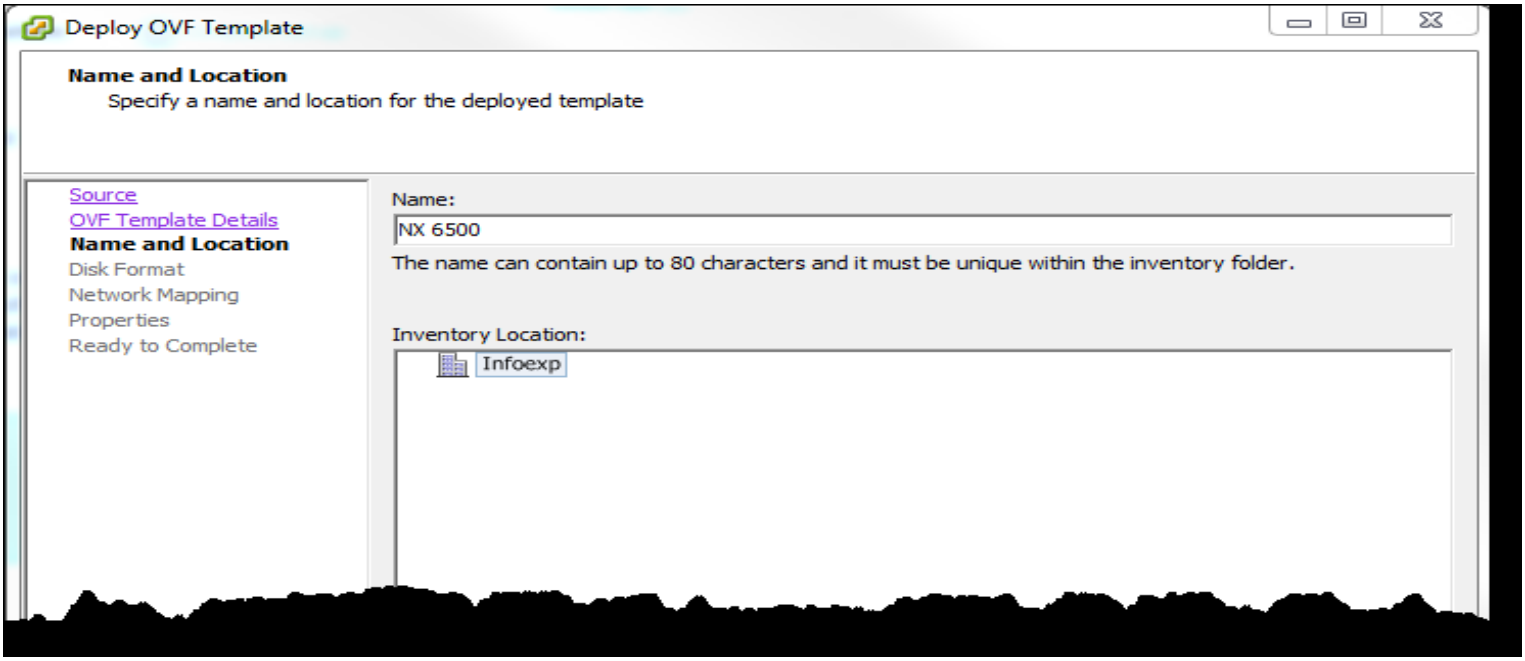
  - On the Source screen, paste the URL that Trellix FireEye provided that points to the OVA file containing the Central Management System, or File Protect system image, or click Browse and navigate to the OVA file stored in your file system, and then click Next.



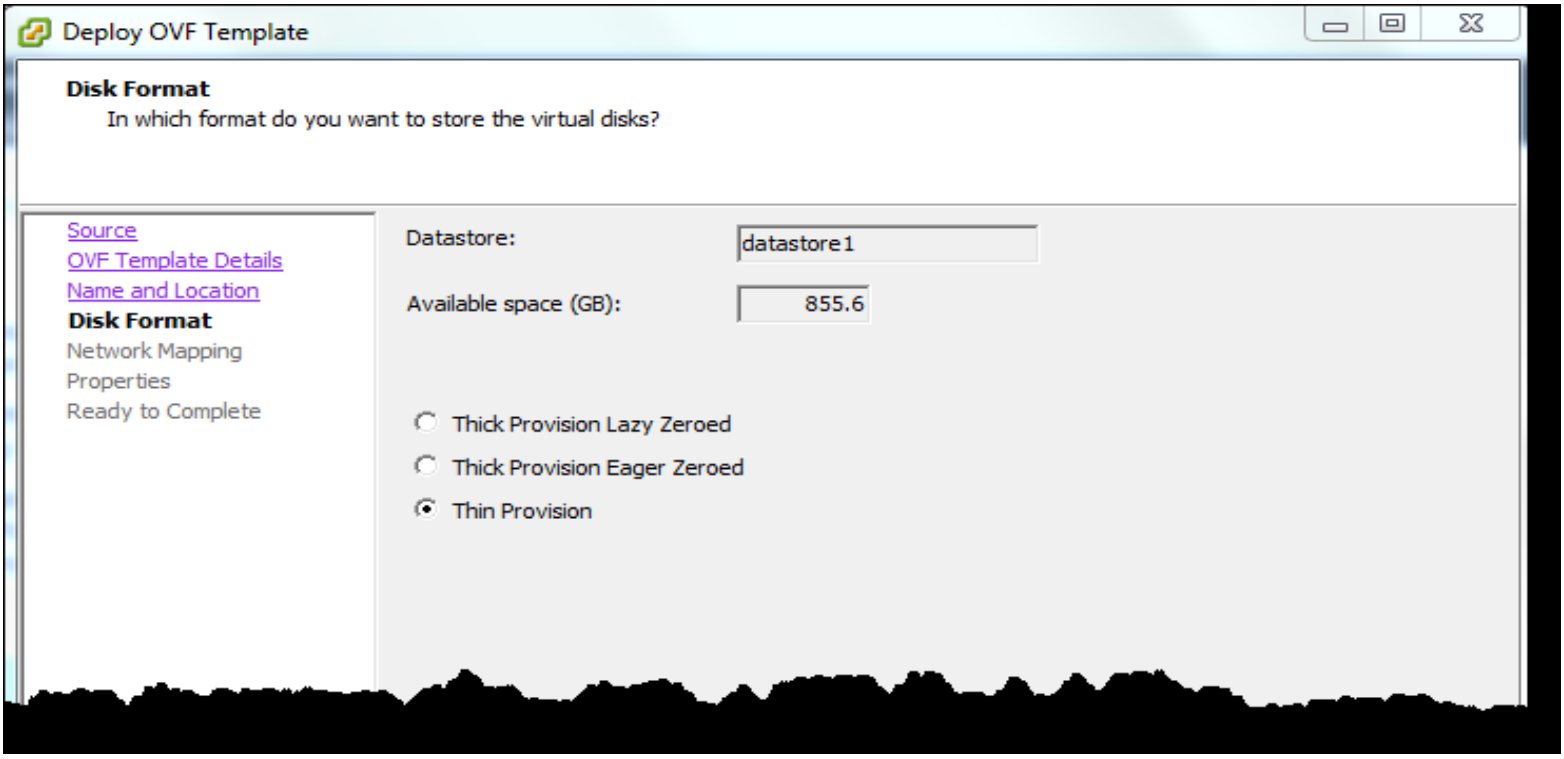
- On the OVF Template Details screen, review the information. If the information is correct, click Next. Otherwise, click Back and enter the correct URL or path.



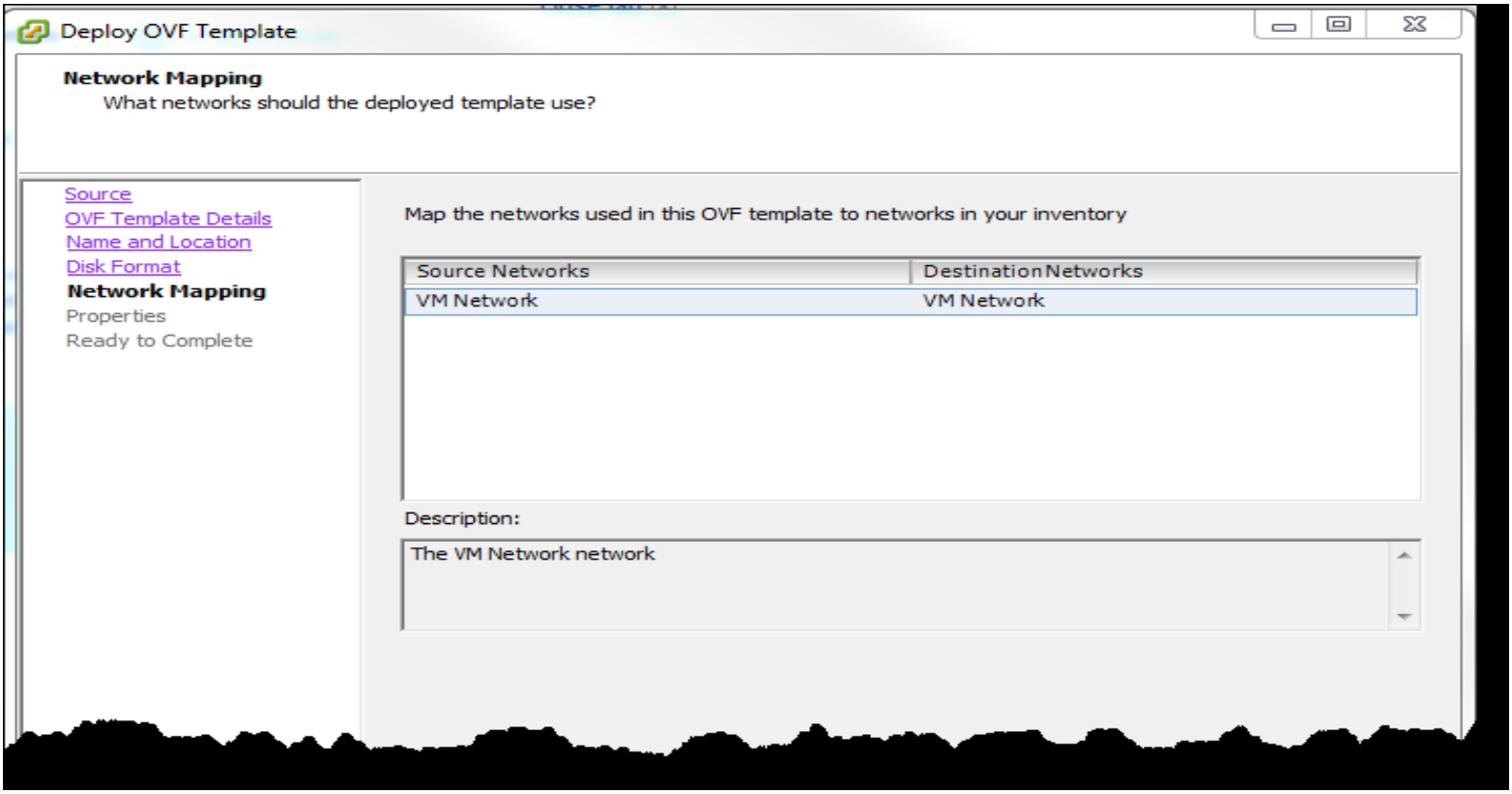
- On the Name and Location screen, enter a unique name that describes the virtual appliance.



- On the Disk Format screen, select Thin Provision, and then click Next.

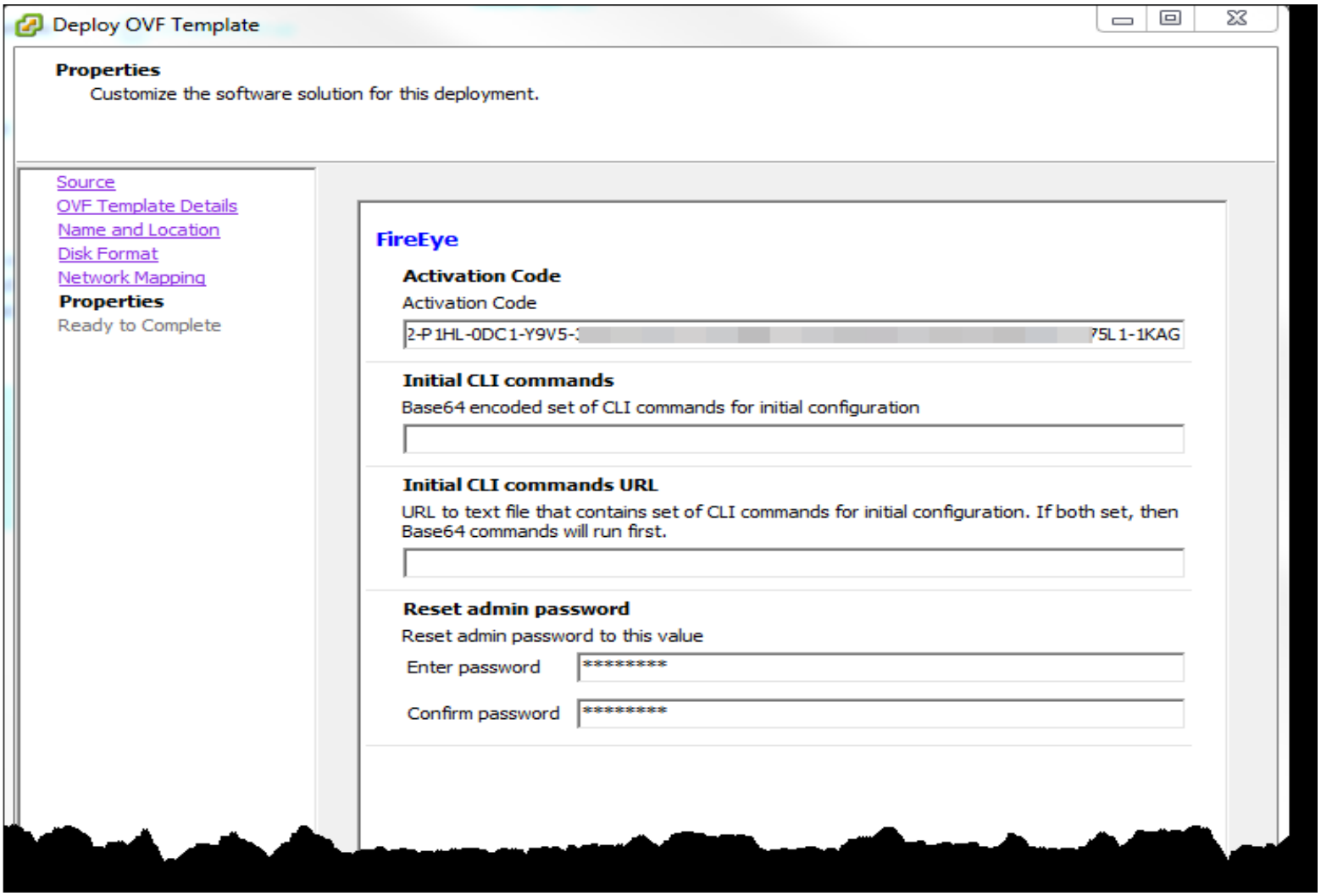


- On the Network Mapping screen, click Next to accept the default settings.



- On the Properties screen, you can complete fields to configure initial settings as described in Using the properties screen.

  (If you do not use this screen, you must type the values into the vSphere Client console manually, because you cannot paste into this console.)



- On the Ready to Complete screen:
  - Verify the information.
  - (*Optional*) Select the Power on after deployment check box.
  - Click Finish.

Note: You can use the system virtual bootstrap reset command to reset the Properties screen values after the virtual appliance is deployed and running.

To perform the initial configuration of a virtual appliance:

1. Log in to vSphere client.

2. In the left pane, expand the ESXi IP address and then select the virtual appliance.

3. Click the Console tab.

4.At the login prompt, enter admin.

5. At the password prompt, enter admin.

6. If prompted to change the password, configure a new password using the `username admin password <new password>` command. You will be logged out. Log in again with the new password.

3 Enabling CC-NDcPP Compliance Mode

A FireEye appliance can be enabled to be compliant with the Network Device Collaborative Protection Profile (NDcPP) by either the command-line interface (CLI) or the web user interface (UI).

Use the command-line interface to enable CC-NDcPP compliance, which performs the following:

- Configures the certified cryptographic components.

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:

```
ssh –c aes128-ctr admin@xxx.xxx.xxx.xxx
```

Otherwise, the connection might fail because the ciphers are incompatible. For example, you could see an error message like the following:

no matching cipher found: `aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes128-ctr`

Note: Running compliance apply after upgrade ensures that all new criteria or modified criteria are enforced. Upgrade does not automatically reapply compliance.

3.1 Enabling CC-NDcPP Compliance Mode Using the Web UI[1]

To enable CC-NDcPP compliance using the Web UI:

- On the Web UI, select the Settings tab.
- Select Compliance on the sidebar.
- Click Enable FIPS + CC Compliance.
- Click Reboot Now.
- Check that there are tick icons in the FIPS column and CC-NDcPP columns on the settings in compliance page.

3.2 Enabling CC-NDcPP Compliance Mode Using the CLI

To enable CC-NDcPP compliance using the CLI:

- Enable the CLI configuration mode:

```
hostname > enable
hostname # configure terminal
```

- Bring the system into CC-NDcPP compliance:

```
hostname (config) # compliance apply standard all
or
hostname (config) # compliance apply standard cc-ndcpp cipher-level
```

[1] VX series appliances don't support WEB UI feature

```
compliant-security
```

- Save your changes:

```
hostname (config) # write memory
```

- Restart the appliance:

```
hostname (config) # reload
```

- Verify that the appliance is compliant:

```
hostname (config) # show compliance standard all
Compliance criterion                          FIPS      CC-NDcPP
-------------------------------------------------------------------------------
Audit logging                                 yes       yes
Boot manager password                         yes       yes
CA Certificates verified                      -         yes
Compliance configuration protection           -         yes
Cryptography run in FIPS mode                 yes       yes
DTI client                                    yes       yes
DTI HTTP proxy                                yes       yes
File transfer protocols                       yes       yes
HTTPS client                                  yes       yes
HTTPS server                                  yes       yes
Image Hotfixes                                yes       yes
IPMI                                          yes       yes
IPsec                                         yes       yes
Kernel security mitigations                   yes       yes
LDAP authentication                           yes       yes
Local password security                       -         yes
Login attempts                                -         yes
Manual key configuration                      yes       yes
NTP                                           -         yes
OpenID connect authentication                 yes       yes
RADIUS authentication                         yes       yes
Restricted licenses                           yes       yes
Random number generator                       yes       yes
SAML authentication                           yes       yes
Secure channel logs                           -         yes
SMTP                                          yes       yes
SNMP                                          yes       yes
```

```
SSH client                                yes       yes
SSH for CMS                               yes       yes
SSH minimum key length                    yes       yes
SSH known host keys                       yes       yes
SSH server                                yes       yes
SSL certificates                          yes       yes
System model                              yes       yes
Remote syslog encryption                  yes       yes
TACACS+ authentication                    yes       yes
User key access                           -         yes
X509 certificate authentication           -         yes
```

Above CSPs details are as follows:

- Audit logging

Ensures audit logging and all log local and remote receivers of logs are at logging minimum of log level NOTICE (either NOTICE, INFO or DEBUG).

- Boot manager password

Disables boot time access to the system boot manager facility (which otherwise could be used by customer service for troubleshooting with a special password).

- CA Certificates verified

Enforces that all trusted X.509 TLS certificates used by the appliance's supplemental CA trust list are in a verified state. Certificates that are not currently verified are removed from the trusted CA list.

The appliance web server certificate must also be verified for compliance. A certificate can fail verification for these reasons:

  - Start or Expiration dates not met
  - Basic Constraints flag not true
  - Certificate Purpose inappropriate for a web server

- Compliance configuration protection

Ensures that any attempt to an unverified certificate to the CA trust list or to the web server is rejected.

- Cryptography run in FIPS mode

The appliance is configured to run and is currently running with the FIPS crypto module enabled. Non-compliant algorithms are rejected if attempted by any software in the management plane.

- DTI client

Ensures that all communications with Trellix Cloud Services (DTI Servers) are configured to use

compliant cipher lists, TLS version 1.2, and enable server certificate verification.

- DTI HTTP proxy

Ensures the system is not configured to use a DTI proxy server. Direct connection to the Trellix Cloud is required.

- File transfer protocols

Ensures that only TLS encrypted protocols are used for all file transfers (disables http and ftp).

- HTTPS client

All HTTPS client requests are configured to use compliant cipher lists, TLS version 1.2, and enforce server certificate verification.

- HTTPS server

All HTTPS services (Web UI, WSAPI) are configured to use compliant cipher lists, TLS version 1.2, and enforce server certificate verification.

- Image Hotfixes

Ensures the current appliance image is not running with a Trellix hotfix patch. While is never expected to compromise compliance in practice, it is a deviation from running a formally certified image, and we cannot be certain whether any given fix will affect certified compliance functions.

- IPMI

Disables the IPMI Ethernet port. IPMI provides back side system monitoring and console access. However, the BMC firmware that implements IPMI services is not part of Trellix's product certification.

- IPsec

Disables IPsec. The IPsec protocol has never been certified on Trellix FireEye products, because very few customers use this feature.

- Kernel security mitigations

Ensures that the kernel is running a version that kernel with microcode that defends against kernel attacks such as Spectre, Meltdown, MDS and other predictive processing kernel attacks.

- LDAP authentication

Ensures LDAP is configured to run over TLS, use compliant cipher lists, TLS version 1.2, and enforce server certificate verification.

- Local password security

Enforces minimum character and length requirements for passwords:

  - password minimum length 15
  - character mix contains at least 1 lower case, one upper case, 1 numeral and 1 special character

- Login attempts

Disables console lockout for the admin user due to too many password attempts, to ensure that the administrator cannot be locked out of the console by an attacker.

- Manual key configuration

Prevents entering keys manually on the physical console. Applies to X.509 and SSH keys.

- NTP

Requires that NTP use a sha1 key for all peers and servers.

- OpenID connect authentication

Ensures that OIDC web policy is configured to either 'allowed' or 'disabled' (not 'required'). This ensures that OIDC is not the only means of authentication to the Web UI, which if so, would lock out other methods.

- RADIUS authentication

Ensures AAA RADIUS services are disabled, as this is not a compliant protocol.

- Restricted licenses

Disables use of the Trellix Restricted License Key. This key is only available to Customer service, but it is used to gain shell access for troubleshooting an appliance. A temporary override of this criterion may be needed in order for customer service personnel to debug a problem (see the compliance options commands).

- Random number generator

Ensures the system is running Trellix's certified entropy kernel module.

- SAML authentication

Ensures that SAML web policy is configured to either 'allowed' or 'disabled' (not 'required'). This ensures that OIDC is not the only means of authentication to the Web UI, which would lock out other methods. Also ensures SAML is configured to use compliant cipher lists, TLS version 1.2, and server certificate verification.

- Secure channel logs

Ensures that all compliance audit log messages regarding secure channel protocols over TLS and SSH appear in the logs.

- SMTP

Ensures the system email client used for event notifications is configured to run over TLS, use compliant cipher lists, TLS version 1.2, and enforce server certificate verification.

- SNMP

Ensures SNMP is only configured to run version 3, and that SNMP password hashes only use SHA has rather than MD5.

- SSH client

Ensures all SSH clients use SSHv2, session rekey limits, and compliant cipher lists, MACs and KEX algorithms.

- SSH for CMS

Ensures the CMS SSH client uses SSHv2, and compliant cipher lists, MACs and KEX algorithms.

- SSH minimum key length

Ensures the ssh protocol (including for CMS SSH) uses strict hostkey checking (a prerequisite) and that both client and server use a minimum.

key length of 2048 bits for RSA keys.

- SSH known host keys

Ensures ssh configuration for CMS CMC connections enforces strict hostkey checking using the system's global known hosts file.

- SSH server

Ensures the SSH server uses SSHv2, session rekey limits, and compliant cipher lists, MACs and KEX algorithms.

- SSL certificates

Ensures trusted certificates used by all management applications have a minimum key length of 2048 bits for RSA and 384 bits for ECDSA certificates, and that only certificates with one of the following secure public signature hash algorithms are used:

  - sha256WithRSAEncryption
  - sha384WithRSAEncryption
  - sha512WithRSAEncryption
  - ecdsa-with-SHA384
  - ecdsa-with-SHA256

- System model

Ensures that the system model on which the firmware is installed is a supported and certified model.

- Remote syslog encryption

Ensures that every remote logging host that receives syslog messages adheres to the following configuration: Transmission over TLS 1.2 a compliant TLS cipher list certificate verification enforced timestamp format uses RFC-3164 format rather than RFC-3339. This ensures full year/month/day/hours/minutes/seconds format e.g.: 2024-07-06T03:51:39.

OSCP enabled, and if there is a defined OSCP responder, a default URL is defined for that responder syslog matches based on IP address of the syslog server if an IP address is used instead of a hostname for the syslog recipient.

- TACACS+ authentication

Ensures AAA TACACS services are disabled, as this is not a compliant protocol.

- User key access

Disables access to user keys from SCP and SFTP so they cannot be exported from the appliance by an authorized admin user. This is to ensure their local security and prevent reuse elsewhere.

- X509 certificate authentication

Ensures that all X.509 certificate-based authentication is CC-NDcPP compliant, namely the following:
Client certificate authentication by the web server is either disabled or allowed (not required). This ensures that the web UI is not the only means of authentication to the Web UI, which if so, would lock out other methods.
Requires that client certificates used to authenticate to the web UI must have the basic constraints flag enabled. If OCSP is enabled, require that a CRL certificate file is defined, to ensure certificate revocation enforcement.
For CAC/PIV client certificate authentication (single sign-on), ensure that authentication is required once for every web UI session.

3.3 Details of CC Mode

Once NDcPP compliance is enabled below settings will be applied by default without any additional configuration

changes.

- Appliance provides AES encryption/decryption in CBC, CTR an GCM mode with 128-bit and 256-bit keys.
    - AES is implemented in the following protocols: TLS and SSH
- Appliance supports signature generation and verification for RSA (2048 and 3072 bits) and ECDSA (P-256, P-384, P-521), in accordance with FIPS PUB 186-4.
    - RSA signature generation and verification are used for the TLS and SSH protocols
    - ECDSA signature verification is used in TLS
- Appliance provides DHG14(2048 bits) key generation in support of DH key exchanges as part of TLS.
- Appliance provides key generation for DHG14 (2048 bits), DH16 (4096 bits), and DH18 (8192 bits) in DH key exchanges used in SSH.
- It provides cryptographic hashing services for key generation using SHA-1, SHA-256, SHA-384, and SHA-512 as specified in ISO/IEC 10118-3:2004.
    - NTP – SHA1
    - TLS and SSH - SHA1, SHA-256, SHA-384 and SHA-512
    - Digital signature verification as part of trusted update validation - SHA-256
    - Hashing of passwords in non-volatile storage - SHA-512
    - Conditioning entropy data – SHA-512
- Appliance implements HMAC message authentication. HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 are supported with cryptographic key sizes of 160, 256, 384, and 512 bits and message digest sizes of 160, 256, 384, and 512 bits.
    - HMAC is implemented in the following protocols: TLS and SSH
- The server supports TLS protocol version 1.2 (rejecting any other protocol version, including SSL 2.0, SSL 3.0 and TLS 1.0, TLS 1.1 and any other unknown TLS version string supplied).
- Appliance provides NIST-approved CTR_DRBG(AES-256) and HMAC_DRBG(SHA-512), as specified in SP 800-90A for RNG functionality.
- The Appliance provides the following public key algorithms for SSH.
    - ssh-rsa (RSA with SHA-1), rsa-sha2-512, rsa-sha2-256

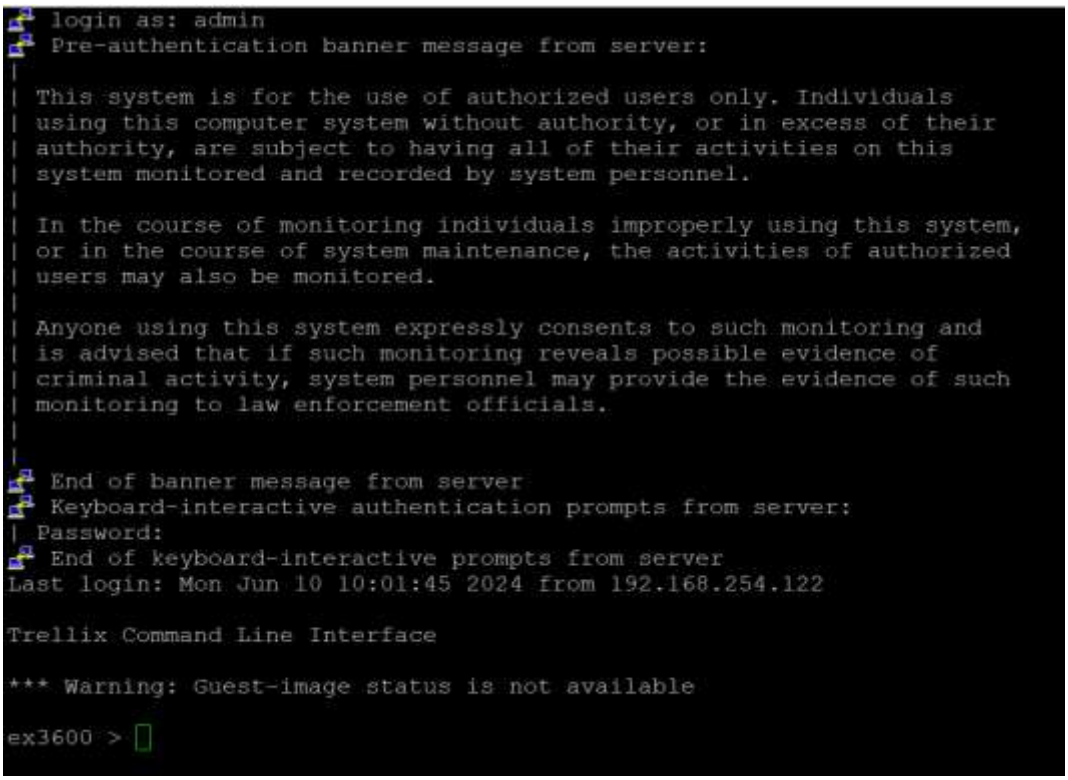
4 TOE Administration

Only authorized administrators can update and modify TOE functions.

4.1 Connect to Appliance via SSH

The FireEye appliance can be managed using SSHv2.To access the CLI of the appliance using the SSH, follow these steps:

- Open a terminal program on your system, such as Putty.
- Enter appliance IP address i.e. IP ass assigned to the ether1.
- When prompted, enter your username and password.



Note: On the first system setup, as a preliminary step, we require that the admin password to be changed.

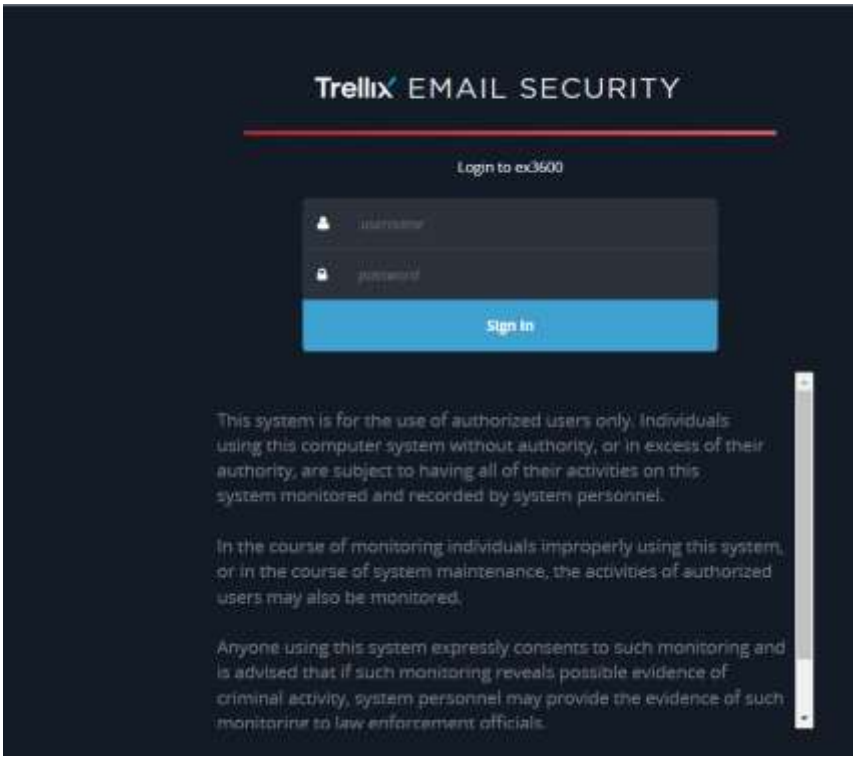
Note: The CLI of the appliance can be accessed using Public Key Authentication.

- For accessing the appliance using Public Key Authentication refer section 4.9 “Configuring SSH Public Keys”.
- Whenever Authentication fails, TOE logs message “User test failed to login via ssh2:” with fingerprint of that key and proceed further with password-based authentication as a fallback mechanism.

4.2 Connect to Appliance via WEB UI[2]

The FireEye appliance can be managed using HTTPS/TLS. The WEB UI is available after the initial setup through the serial console:

- Launch a web browser from a laptop that is network-connected.
- Point the browser at the same IP address that was assigned to the ether1 followed by /login (for example, https://a.b.c.d/login).
- On the sign-in page, enter the administrator username and password. Then click **Sign In**.

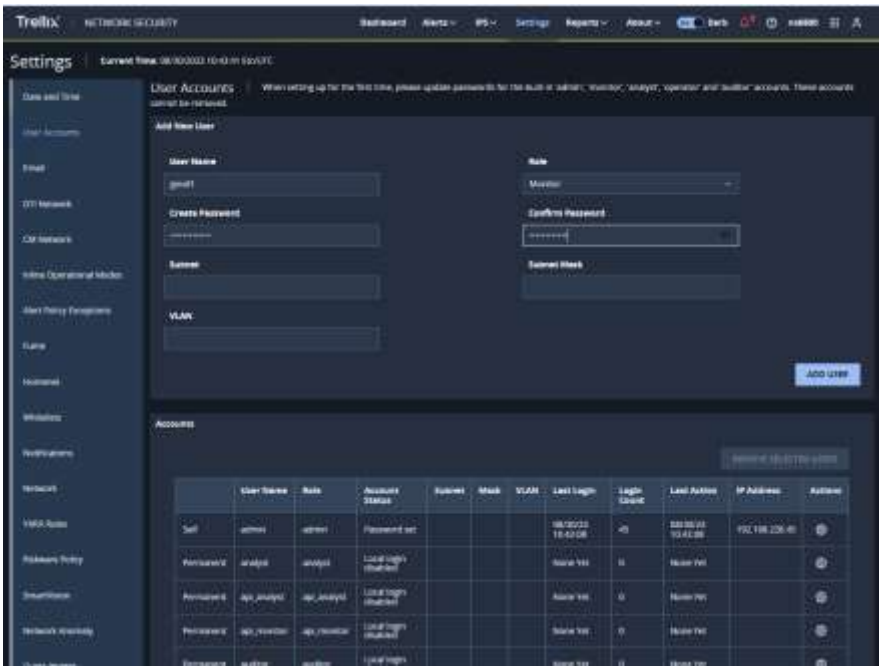


4.3 User Creation via the Web UI[3]

Use the **User Accounts** page from settings to configure new users for the TOE.

[2] VX series appliances don't support WEB UI feature

[3] VX series appliances don't support WEB UI feature



Note: The VX series models do not support the Web UI feature; therefore, the GUI/HTTPS logon method is not available on these models.

4.4 User Creation via the CLI

Create or remove a user account. New users are created initially with admin privileges and disabled. To enable a user account, just set a password on it.

```
username <userid> password {0, 7} <password>
```

Removing a user account terminates any active logins of that account, in either the CLI or Web UI.Note that usernames have a length limit of 31 characters.

```
[no] username <userid>
```

This removes all existing roles from the account and replaces them with the specified one. The "no" variant removes all roles from the account.

```
username <userid> role <role>
```

```
no username <userid> role
```

The "username <userid> password ..." commands set a password on the account. The variant with no number after the word "password" takes a plaintext password, and the variant with a "0" is exactly the same. The variant with a "7" accepts the password in the same hashed form in which it is stored in the password file. This is useful for the 'show configuration' command, since the cleartext password cannot be recovered after it is set, so this is the only way to reconstruct the configuration.

If the password is omitted with the cleartext forms of this command, the user will be prompted for the password. The entry will be echoed as '*' characters for security reasons, and the same string will be required to be entered twice, for confirmation.

The "`username <userid> disable`" command makes the account act as though it did not exist.

There will be no way to log into the account, as the base operating system will not know about it at all. It will also not be possible to map remotely authenticated users to this account -- if you want to do that, use "username <userid> disable login" instead. The "no" variant reverses this procedure, and leaves the account in the same state it was in before it was disabled.

"username <userid> disable login" locks out access to an account. There will be no way to log into that account, but unlike a fully "disabled" account, it will still be usable as a local account for mapping remotely-authenticated users to.

Disabling or locking out an account (the previous two commands described) logs off any open sessions of that user, just as deleting the user account does (see "no username <userid>" above for details).

The "username <userid> disable password" command forbids login to the account using a local password.

The "username <userid> disable local-login" command forbids login to the account using any local login mechanism.

The "no" variants of the above three commands (locking out an account, or disabling password login) do not actually undo these commands, as the old password which was previously set cannot be recovered. Instead, they simply print out a message explaining this, and what the other options are.

Those commands which set the hashed password on the local account (all of these except "[no] username <userid> disable") are subject to the configuration setting set by "aaa authentication password local change require-current non-admin". If that flag is enabled, any locally authenticated user without administrative privileges who is trying to set the password on their own account is required to provide their current password before setting a new one. They may provide it on the command line using the "curr-password" option; or if it is not provided, they will be prompted for it. If the provided password is incorrect, the change is not permitted. If the configuration setting is not enabled (so the current password is not required), but it is provided on the command line anyway, it will still be validated, and the password change will still not go through if it is incorrect. Note that even if using the "7" option to provide an encrypted (hashed) password, it is still a plaintext version of the current password that is required for verification.

The following commands are used to handle password configuration and enabling / disabling of user login.

```
username <userid> password [<cleartext password> [curr-password
<current cleartext password>]]

username <userid> password 0 [<cleartext password> [curr-password
<current cleartext password>]]

username <userid> password 7 <encrypted password> [curr-password
<current cleartext password>]

username <userid> nopassword [curr-password <current cleartext
password>]

[no] username <userid> disable

[no] username <userid> disable password [curr-password <current
cleartext password>]

[no] username <userid> disable login [curr-password <current cleartext
password>]
```

```
[no] username <userid> disable local-login [curr-password <current
cleartext password>]
```

Display a list of all currently logged-in users, and related information such as idle time and what host they have connected from.

```
show users
```

Like "show users", except that instead of Line, Host, and Idle time, this displays the set of roles the login session has. Normally this will be the same as the roles assigned to the user account in configuration, as would be seen from "show usernames roles". But if the authentication server returned additional role strings to be granted to the user (and if the system is configured to accept such roles), they would be listed here.

```
show users roles
```

Display a list of all user accounts, along with the full name, role, and account status.

```
show usernames
```

Display full information about the specified user account. In addition to what is currently displayed in columnar format for "show usernames", this will also include the age of this user's password, and whether or not they will be required to change their password on next local password login.

```
show usernames user <username>
```

4.4.1 User Roles

The TOE implements role-based access control. Administrative users are required to login before being provided with access to any administrative functions. The TOE supports several types of administrative user roles. Collectively these roles comprise the Security Administrator. The supported roles include:

- Admin: The system administrator is a “super user” who has all capabilities. The primary function of this role is to configure the system.
- Monitor: The system monitor has read-only access to some things the admin role can change or configure.
- Operator: The system operator has a subset of the capabilities associated with the admin role. Its primary function is configuring and monitoring the system.
- Analyst: The system analyst focuses on data plane analysis and possesses several capabilities, including setting up alerts and reports.
- Auditor: The system auditor reviews audit logs and performs forensic analysis to trace how events occurred.

Each of the predefined administrative roles has a set of permissions that will grant them access to the TOE data, though with some roles, access is limited.

The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to all privileged levels.

4.5 Authentication Failure Handling

The locking mechanism can be configured to remain locked until an administrator unlocks the account, or it can be configured to unlock after a specified period of time.

To configure, it requires following commands:

1. Configure the number of failed attempts or lockout time in accordance with your organization's policies (this setting is automatically applied to all administration interfaces):

   ```
   hostname (config) # aaa authentication attempts lockout max-fail <count>
   ```

   Note: The configurable range of failed attempts is between 1 to 15 attempts.

   ```
   hostname (config) # aaa authentication attempts lockout unlock-time <time in seconds>
   ```

   Note: If the unlocking mechanism is automatically applied after a specified time period, then the user account will be unlocked when the specified number of seconds have elapsed since the locking mechanism was engaged.

2. To unlock an account before lockout period elapses, following command is required:

   ```
   hostname (config) # aaa authentication attempts reset
   ```

Note: Locally connected administrators are not subject to the lockout as the locking mechanisms apply to authentication attempts through both SSH and the GUI[4]. The failed authentication lockout does not apply to the local console, ensuring administrative access is always available.

Irrespective of whether an administrator intervened or whether the elapsed time occurred, when a locked account is unlocked, the failure counter associated with that user is reset to 0.

If a user succeeds at authenticating before the locking mechanism has been enabled, the failure counter is reset to 0.

If the lockout attempts are set to, for example, 5 attempts, then the user will be locked out after the 5th consecutive failed login attempt. This means that the 6th and subsequent attempts will fail to gain access to the TOE even if the credential being offered is correct.

Regardless of method of administering the TOE, the user is presented with an authentication prompt. At the authentication prompt the username of the administrator and credential (either password or SSH key) must be presented. Administration is available only after the correct username/credential combination is presented.

4.6 Password Management

Passwords can be composed of any combination of upper and lower case letters, numbers, and special characters that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "'", "+", "-", ".", "/", ":", ";", "<", "=", ">", "?", "[", "\", "]", "^", "_", "`", "{", "|", "}", and "~".

The TOE can configure 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 strong passwords, following commands are required:

[4] VX series appliances don't support WEB UI feature.

```
aaa authentication password local character-type lower-case minimum
<count>
aaa authentication password local character-type upper-case minimum
<count>
aaa authentication password local character-type numeral minimum
<count>
aaa authentication password local character-type special minimum
<count>
```

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

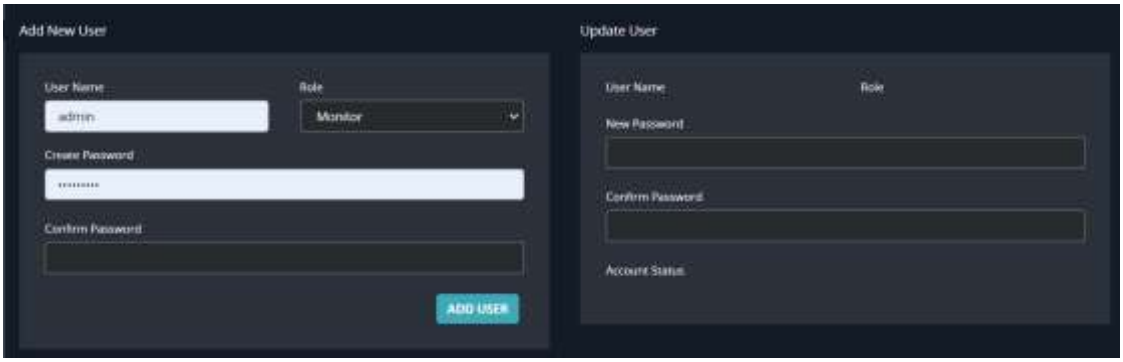
```
aaa authentication password local length minimum <count>
```

Note: It has a range of 8 to 32 characters. In CC mode of operation, the minimum length is 15 characters.

4.6.1 Resetting Passwords[5]

Resetting User Password from GUI:

- Navigate to the **User Accounts** page from **Settings** to reset the password for users.
- Enter the Name of the user in the **Username** field and entry the password in the **New Password** and **Confirm Password** fields.



Resetting User Password from CLI:

Run the below command to reset the user passwords:

```
Hostname (config) # username XXXX password XXXXX
```

4.7 Protected Authentication feedback

The TOE does not provide any feedback for the password characters entered. This is by default and does not require any configuration.

[5] VX series appliances don't support WEB UI feature

4.8 Remote SSH Administration

Enable or disable the ssh server. If the ssh server is disabled, the CLI is only accessible over the serial console. Note that this does not terminate existing ssh sessions; it will only prevent new ones from being established.

```
[no] ssh server enable
[no] ssh server rekey enable
```

SSH server rekey limit configuration. Enables and sets data and time limits when the server will force the session key to be renegotiated.

```
ssh server rekey data-limit <data limit in MB>
ssh server rekey time-limit <time limit in seconds>
```

Note: time limit is not more than one hour, and data limit is one gigabyte.

The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey. All session keys are rekeyed at the same time (e.g. confidentiality and integrity keys).

Set the minimum version of the SSH protocol that the servers support. 1 and 2 is allowed but the only valid value is 2 for CC-NDcPP compliance.

```
ssh server min-version 2
no ssh server min-version
```

Minimum SSH key length. Any keys smaller than this will not be accepted. Existing keys with length smaller than this are dropped. Existing host-keys smaller than this are dropped then regenerated. The default is 2048.

```
ssh server min-key-length <number of bits>
no ssh server min-key-length
```

Regenerate new host keys for the ssh server. This generates three keys: RSA for sshv1, RSA for sshv2. Note that the system automatically generates the host keys on its first boot, so this only needs to be done if a security breach is suspected and the keys need to be changed.

```
ssh server host-key generate
```

Manually set the host-key (either private or public but should be both if changing) of the specified key type. If the positive form of the private key command is used with no key, the user will be prompted for the key. Any entries made at this prompt will only echo with the '*' character, and the user will have to enter the same string twice for confirmation.

```
ssh server host-key <type> private-key [<key>]
ssh server host-key <type> public-key <key>
```

4.9 Configuring SSH Public 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.

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

Note: For CC compliance, SSH public-key based authentication implementation uses ssh-rsa, rsa-sha2-512 and rsa-sha2-256 as its public key algorithms and rejects all other public key algorithms. No configuration is required apart from enabling CC-NDcPP compliance.

2. Save your changes:

```
hostname (config) # write memory
```

Use the commands in this section to create a new host key for SSH user authentication:

1. To configure minimum key length, following command is required:

```
hostname (config) # ssh server min-key-length <key length>
```

2. To generate server Host Key, following command is required:

```
hostname (config) # ssh server host-key generate
```

To configure the TOE to support RSA based SSH authentication method.

```
SSH server host-key <rsa2> public-key '<public key generated by server>'
```

4.10 Configuring X.509 certificate Authentication for the Web UI[6]

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

```
hostname (config) # crypto certificate signing-request generate
```

The above command generates a CSR without the optional common name. To generate aCSR with a common name, the request must be made with the following option,

`Name` – This is the common name of the device

`Organization` – This is the associated organization

`Org-Unit` – This is the associated organizational-Unit

`Country-Code` – This is the associated Country

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

```
hostname (config) # crypto certificate name <name of the certificate>
public-cert match csr <name of the CSR> pem <quoted PEM string>
```

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

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

```
hostname (config) # no crypto certificate signing-request csr-name XXX
```

4.11 Addition and Removal of Certificates from Trust Store

[6] VX series appliances don't support WEB UI feature

4.11.1 Addition of Certificates to Trust Store

To add certificates using web UI:

- On the Web UI, select Settings Tab
- Select Certificates/Keys
- Click Add Root/Intermediate CA Certificate
- Choose file then commit

To add certificate using CLI:

```
hostname (config) # crypto certificate name xxx public-cert pem
xxx
hostname (config) # crypto certificate ca-list default-ca-list
name xxx
```

If a connection is not possible because the validity of a certificate cannot be determined, there is no override option. A valid certificate must be presented. This may include installing required certificates in the trust store.

4.11.2 Removal of Certificates from Trust Store

To remove certificates using web UI:

- On the Web UI, select Settings Tab
- Select Certificates/Keys
- Select the certificate to be deleted
- Select the Action and click on Delete

To delete certificate using CLI:

```
hostname (config) # no crypto certificate name xxx
hostname(config) # no crypto certificate ca-list default-ca-list name
```

4.12 Reverify the web server certificate[7]

In order to maintain full compliance mode, you would need to install an acceptable web server certificate and get it verified.

1. Upload trusted certificate on the device and reconfigure the web server to use your signed/trusted certificate.
    - On the Web UI, select Settings Tab
    - Select Certificates/Keys
    - Add the root certificate that signed your web server certificate to the CA trust list
    - Go to HTTPS configuration tab, upload the trusted web server certificate and activate the trusted

[7] VX series appliances don't support WEB UI feature

certificate

2. Reverify the web server certificate.

```
device (config) # crypto certificate reverify cert-name XXXXX
```

3. Verify that it shows as verified.

```
device (config) # sh crypto certificate name XXXXX
```

4. Reapply compliance.

```
device (config) # compliance apply standard all
```

5. Verify that all CC-NDcPP criteria show as "yes."

```
device (config) # show compliance standard {all|fips|cc-
ndcpp}
```

6. Save configuration.

```
device (config) # write memory
```

4.13 X.509 Certificate[8]

The TOE performs X.509 certificate validation at the following points:

- TOE TLS client authentication of server X.509 certificates.
- When certificates are loaded into the TOE, such as when importing CAs, certificate responses and other device-level certificates (such as the web server certificate presented by the TOE TLS web GUI).

The TOE validates certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TOE validates a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TOE validates the revocation status of the certificate using Online Certificate Status Protocol (OCSP) as specified in RFC 6960.
- The TOE validates the extendedKeyUsage field according to the following rules:
  - 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 shall 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 use X.509 certificates for trusted updates, hence the requirement for Code Signing

[8] VX series appliances don't support WEB UI feature

purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field is trivially satisfied.

Certificate revocation checking is performed on the leaf and intermediate CA certificates using OCSP responders as part of the authentication step. There is no difference in handling of revocation checking during authentication irrespective of whether a full certificate chain or only a leaf certificate is being presented. The OCSP signing certificate must have the OCSP signing purpose in the extendedKeyUsage extension.

If, during the entire trust chain verification activity, any certificate under review fails a verification check, then the entire trust chain is deemed untrusted and the TLS connection is terminated, as TLS is only trusted channel. As part of the verification process, OCSP is used to determine whether the certificate is revoked or not. If the OCSP responder cannot be contacted, then the TOE will choose to automatically reject the certificate in this case.

The administrator does not determine the default handling of certificates.

As X.509 certificates are not used for either trusted updates or firmware integrity self-tests, the code-signing purpose is not checked for in the extendedKeyUsage, hence the requirement for Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field is trivially satisfied.

4.13.1 OCSP Server Requirements:

The OCSP Server, provided by the operational environment, must be loaded with

the following certificates:

- Self-certificate (system cert) signed by the issuer (CA authority)
- Root certificate who signed the system certificate
- Root certificate of the client who is trying to initiate the connection

4.14 Logging Out[9]

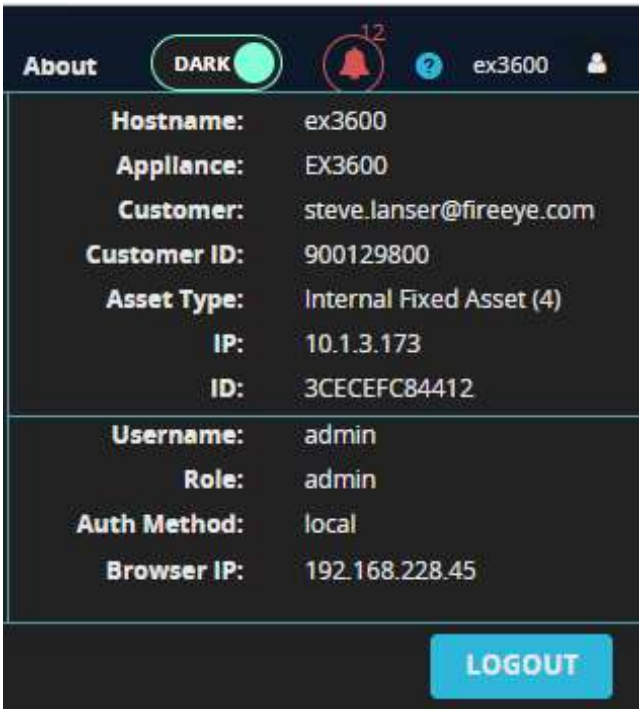
To facilitate ending a session, the administrative user must log out of the TOE.

From the command line use the `exit` command.

```
hostname > exit
```

From the Web UI, select the “Log Out” Option from the administrative interface.

[9] VX series appliances don’t support WEB UI feature


About
DARK
12
ex3600
Hostname: ex3600
Appliance: EX3600
Customer: steve.lanser@fireeye.com
Customer ID: 900129800
Asset Type: Internal Fixed Asset (4)
IP: 10.1.3.173
ID: 3CECEFC84412
Username: admin
Role: admin
Auth Method: local
Browser IP: 192.168.228.45
LOGOUT

5 Using an Audit Server

TOE establishes the trusted channel to the audit server. Use the following procedure to configure an audit server.

5.1 Audit Server Requirements

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

5.2 System Behavior

When configured to use an audit server the FireEye AX, CM, EX, FX, HX, NX, and VX Series Appliances transmit audit events to the audit server at the same time logs are written locally to non-volatile storage. If the connection fails, these appliances continue 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 archive file is deleted to allow a new log to be created so the TOE overwrites previous audit records.

```
logging files rotation criteria frequency {daily, weekly, monthly}
logging files rotation criteria size <log file size threshold>
logging files rotation criteria size-pct <log file size percent threshold>
```

Only Authorized Administrators can clear the local log files, and local audit records are stored in a directory that does not allow administrators to modify the contents.

Configure how many old log files will be kept. If the number of log files ever exceeds this number (either at rotation time, or when this setting is lowered), the system will delete as many as necessary to bring it down to this number, starting with the oldest.

```
logging files rotation max-num <max number of files to keep>
```

Force an immediate rotation of the log files. This does not affect the schedule of autorotation if it was done based on time: the next automatic rotation will still occur at the same time it was previously scheduled for. Naturally, if the autorotation was based on size, this will delay it somewhat as it reduces the size of the active log file to zero.

5.3 Audit Server Configuration

To use an audit server:

- Enter the CLI configuration mode:

  ```
  hostname > enable
  hostname # configure terminal
  ```

- Specify the protocol to log in to the remote host. For example:

  ```
  hostname (config) # logging x.x.x.x protocol tls port 6514
  ```

  where x.x.x.x is the hostname or IP address of a syslog server where you want to send auditing messages. The TLS version is 1.2 by default.

- To enable class-specific overrides of log levels for this sink:

  ```
  hostname (config) # logging x.x.x.x trap override
  hostname (config) # logging x.x.x.x trap info
  ```

- To enable OCSP checking run the below command:

  ```
  hostname (config) # logging remote OCSP enable
  ```

- Save your changes:

  ```
  hostname (config) # write memory
  ```

- Check the status:

  ```
  hostname (config) # show logging
  ```

The device will begin sending audit events to the audit server as soon as the connection is made after the audit server is configured. If the server certificate is invalid, the TSF will by default not create a trusted channel.

For example, a typical configuration for compliance purposes would capture only auditing messages at the notice level and above.

```
Hostname (config) # logging 10.1.3.175 protocol tls port
6514
Hostname (config) # logging 10.1.3.175 trap override
Hostname (config) # write memory
```

Saving configuration file ... Done!

```
Hostname (config) # show logging
Local logging level:                          info (OVERRIDES DISABLED)
   Override for class pcp_mip_jabe:           info
   Override for class mgmt-back:              info
   Override for class mgmt-front:             info
   Override for class mail:                   info
Remote syslog default level:                  notice
Remote syslog servers:
   10.1.3.175                                 notice
      protocol:                               tls
      port:                                   6514
   SSL min version:                           tls1.2
   SSL cipher list:                           fips-and-cc-ndcpp
   verify peer certificate:                   yes
```

```
   OCSP enabled:                                yes
   Default OCSP URL:
   OCSP override responder:                     no
Receive remote messages via UDP:                no
Receive remote messages via TCP:                no
Receive remote messages via TLS:                no
Log file rotation:
   Log rotation size threshold:                 1 megabytes
   Archived log files to keep:                  5
Log format:
   Timestamp format:                            rfc-3339
   Subsecond timestamp field:                   disabled
Secure channel logs:                            yes
```

TOE restricts the ability to modify the behavior of transmission of audit data to an external IT entity (OCSP responder, TLS ciphersuites), and handling of audit data (number of logs to retain) to Security Administrators.

5.4 Auditable Events

5.4.1 Format

The following is the general format of all syslog messages:

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

Field details are as follows:

Timestamp: The date and time when the message was generated, indicating when the event occurred.

Hostname: The name device that generated the message, identifying the source of the log.

Process name[pid]: The name of the process and its process ID that generated the message, specifying which software component is logging the message.

[subsystem.priority]: Indicates the facility (subsystem) and the severity level (priority) of the message, providing context about the source and importance of the log.

Message content: The actual log message detailing the event or condition being reported.

For example, a locally logged message looks like this:

```
2020-08-9T08:11:58 fireeye-Appliance pm[5916]: [pm.NOTICE]: AUDIT: System
initialization completed
```

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

```
2020-08-9T08:11:58 fireeye-Appliance 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:

```
2020-08-9T13:14:47 fireeye-Appliance mgmtd[8642]: [32887.144] [mgmtd.NOTICE]:
AUDIT: User login: username 'acumensec', role 'admin', client 'CLI', line
'pts/0', remote address '10.1.2.157', auth method 'local', auth submethod
'password', session ID 4586
```

5.4.2 CC-NDcPP Events

A. Start-up of the audit functions

B. Shut-down of the audit functions

```
2024-06-04T01:09:38 ex3600 mgmtd[7386]: [mgmtd.NOTICE]: AUDIT: Shutting down system logger
2024-06-04T01:09:43 ex3600 logger: Process Manager service command: stop
```

C. Administrative login

```
2024-06-06T07:38:28 ex3600 sshd[5305]: User admin (System Administrator) logged in via ssh2 from 10.1.3.175
2024-06-06T07:38:28 ex3600 cli[5343]: [cli.NOTICE]: user admin: CLI launched
2024-06-06T07:38:28 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: User admin (local user admin) authentication method: local (pa
ssword)
2024-06-06T07:38:28 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: User login: username 'admin', full name 'System Adminis
trator', role 'admin', client 'CLI', line 'pts/0', remote address '10.1.3.175', auth method 'local', auth submethod 'p
assword', session ID 488357
```

D. Administrative logout

```
2024-06-06T07:37:41 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: User logout: username 'admin', full name 'System Admini
strator', role 'admin', client 'CLI', line 'pts/0', remote address '10.1.3.175', auth method 'local', auth submethod '
password', session ID 487581
2024-06-06T07:37:41 ex3600 cli[1981]: [cli.NOTICE]: AUDIT: user admin: CLI exiting
```

E. Changes to TSF data related to configuration changes

a. Time Change:

```
2023-05-19T11:16:12 ex3600 cli[9580]: [cli.NOTICE]: AUDIT: user admin: Executing command: sh clock
2023-05-19T11:16:38 ex3600 cli[9580]: [cli.NOTICE]: AUDIT: user admin: Executing command: clock set 15:0:0
2023-05-19T11:16:38 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: requested by: user admin (System Administrator) via CLI
 (session ID 222288)
2023-05-19T11:16:38 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: descr: system clock: set time
2023-05-19T11:16:38 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: param: time of day: 15:00:00
2023-05-19T15:00:00 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: status: completed with success
2023-05-19T15:00:00 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Time change detected, clock was moved 3h 43m 21.167s forward
```

b. Addition of certificate:

```
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 1: System global default CA certificate 4 added
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 2: System global default CA certificate 4: CA certifi
cate name initially set to "ICA"
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 3: The subject hash e81b420b of a default CA list cer
tificate added
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 4: The cert_id wildcard of a default CA list certific
ate with subject hash e81b420b cert_id be620044391a3551e2107ca0201b82458eebd150 added
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 5: The cert_id wildcard of a default CA list certific
ate with subject hash e81b420b cert_id be620044391a3551e2107ca0201b82458eebd150: CA subject hash ordinal symlink number initially set to 0
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 6: The cert_id wildcard of a default CA list certific
ate with subject hash e81b420b cert_id be620044391a3551e2107ca0201b82458eebd150: Default CA list cert_id initially set to "be620044391a3551e2107ca
0201b82458eebd150"
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 7: The cert_id wildcard of a default CA list certific
ate with subject hash e81b420b cert_id be620044391a3551e2107ca0201b82458eebd150: Default CA list cert_name initially set to "ICA"
```

c. Removal of certificate:

```
2023-09-14T09:09:26 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4785: item 1: Certificate name ICA, ID be620044391a3551e2107ca020
1b82458eebd150 deleted
2023-09-14T09:09:26 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4785: item 2: Certificate ID be620044391a3551e2107ca0201b82458eeb
d150: CA certificate chain member was "false" before deletion
2023-09-14T09:09:26 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4785: item 3: Certificate ID be620044391a3551e2107ca0201b82458eeb
d150: Certificate name was "ICA" before deletion
```

F. Generating/import of cryptographic keys

```
2024-07-17T18:11:57 ex3600 cli[19160]: [cli.NOTICE]: AUDIT: user admin: Executing command: crypto certifi
cate signing-request csr-name test generate
2024-07-17T18:11:57 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Action ID 634514: requested by: user admin
 (System Administrator) via CLI (session ID 11425473)
2024-07-17T18:11:57 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Action ID 634514: descr: Generate certific
ate signing request (CSR)
2024-07-17T18:11:57 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Action ID 634514: param: CSR name: "test"
2024-07-17T18:11:57 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Action ID 634514: param: common name (host
name or contact name): ""
2024-07-17T18:11:57 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Action ID 634514: param: CSR key type: "rs
a"
2024-07-17T18:11:57 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Action ID 634514: param: overwrite: no
2024-07-17T18:11:57 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Action ID 634514: param: Subject Alternati
ve Name DNS list: ""
2024-07-17T18:11:57 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Action ID 634514: param: Subject Alternati
ve Name IP address list: ""
2024-07-17T18:11:57 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Action ID 634514: param: Subject Alternati
ve Name URI list: ""
2024-07-17T18:11:57 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Action ID 634514: param: Subject Alternati
ve Name email address list: ""
2024-07-17T18:11:58 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 147899: requested by: use
r admin (System Administrator) via CLI (session ID 11425473), 7 item(s) changed
2024-07-17T18:11:58 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 147899: item 1: Certifica
te signing request (CSR) Name test added
2024-07-17T18:11:58 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 147899: item 2: Certifica
te signing request (CSR) Name test: Certificate signing request comment initially set to ""
```

```
2024-07-17T18:11:58 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 147899: item 2: Certifica
te signing request (CSR) Name test: Certificate signing request comment initially set to ""
2024-07-17T18:11:58 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 147899: item 3: Certifica
te signing request (CSR) Name test: Certificate signing request (CSR) PEM string initially set to "-----B
EGIN CERTIFICATE REQUEST----- MIIEFDCCAnwCAQAwgZIxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlh MREwDwYDVQ
QHDAhTYW4gSm9zZTEQMA4GA1UECgwHVHJlbGxpeDEiMCAGA1UECwwZ VHJlbGxpeCBTZWN1cml0eSBQbGF0Zm9ybTEPMA0GA1UEAwwGZX
gzNjAwMRQwEgYJ KoZIhvcNAQkBFgVhZG1pbjCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGB AMYoBEqf2bC01jsRurxz+lcfO
utFu27c8Y3/zawghbfAnMSYO5FDJis9iSUgK9ga v/W/dvCaxTCJnoViABJoSyWCdOGoQw4prCCGraRQ4q/9xAYm3yAV7Nz0w8ZIxT+L
OiW3v+56DzdjisUPOzIgGYn9kIyrAZ+359Kya7sPpr8lMrug71adVF7B/JtIrcqB ZzDtEPcJGXN8bNLPWRhA0nM4yYwJEJHVNpQFyIWo
IUuxEmwtSjjm2GeCZMnojxiC gIljrzkuVHJ8F7DwKXtkAIkoAR/hwya9z6X6Mk2AKkaRekH1ozsP9Fs59lRq+fsS rloqqa4XZ7GH1pe
yaXIxDCBqJY3zCJUJPdkds2ChqGdn2vSasEiw6o38BuH9DAIF Sx0aORNAuK0kNLPOpHZ2KMO6jH72iEsfdSajN0hDnOSTV1YoZ+N/Qm8
TV9Kx/y3G twl6hR4qFQSRC4YKu1bSXo0Zh9OrgEC1hBqVPA4ZD/hW/0H0hGOGKuIA2cVQu3p4 0wIDAQABoDwwOgYJKoZIhvcNAQkOMS
0wKzAJBgNVHRMEAjAAMAsGA1UdDwQEAwIF 4DARBgNVHREECjAIggZleDM2MDAwDQYJKoZIhvcNAQELBQADggGBACL18riY2XEt Oalyv
4oGgjEHgw3beZ7V1fUGywo7yBWHLtr3aWKZFbKHlxQx5hXcSU9w2r2vyExj yCysjcRQxN9YdWiopBfCT8PkE7FFmuki3RCrO5pH28fwn
nYGp2U9mxh33h6YNw1v lntO+QReyRdaZtCVhyQiFO+y7orGeSKQ+o19xshiScqHCYijgRnh/MmFdTi1ssNs Hy/85m+eXk/6rusMiUHs
s7PztaoTuialzHn7+PYaz6oEs9MXdjc64N/nCKLAyc44 S20jOwFrh/qf3gbTbWxjXYX6XMT/Lskivg2oc+ug0yjQamPsrmAZldwyvQX7
mWLp zgW4QwxY2eAV14/fMQljSuTosHefMhQ3ZiXhoVlBfJp/XafQxqY8kdjVqDgPVbB8 ljCk0JLXJzgakhoDsIZt1jnTE8g56r/h6Tr
JoZD5HN5oY7aypoOhFHLk7XyaUo+e GkBlOcb3g+ZYGK3ULWXMsxyZynW/L9bDmQ1zLoHvNSu7XaD/tLb67w== -----END CERTIFICA
TE REQUEST----- "
2024-07-17T18:11:58 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 147899: item 4: Certifica
te signing request (CSR) Name test: Certificate signing request (CSR) unique ID initially set to "81bb680
ebfd7249163569eeb32a1d38c5b771a2e"
2024-07-17T18:11:58 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 147899: item 5: Certifica
te signing request (CSR) Name test: Certificate signing request (CSR) unique name initially set to "test"
2024-07-17T18:11:58 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 147899: item 6: Certifica
te signing request (CSR) Name test: Certificate signing request (CSR) private key PEM string added
```

G. Deleting of cryptographic keys

```
2024-06-06T07:35:48 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 6584: requested by: user admin (System
 Administrator) via CLI (session ID 487581), 7 item(s) changed
2024-06-06T07:35:48 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 6584: item 1: Certificate signing requ
est (CSR) Name test deleted
2024-06-06T07:35:48 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 6584: item 2: Certificate signing requ
est (CSR) Name test: Certificate signing request comment was "" before deletion
2024-06-06T07:35:48 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 6584: item 3: Certificate signing requ
est (CSR) Name test: Certificate signing request (CSR) PEM string was "-----BEGIN CERTIFICATE REQUEST----- MIIC/zCCAec
CAQAwfjELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWEx ETAPBgNVBAcMCFNhbiBKb3NlMQ8wDQYDVQQKDAZhY3VtZW4xCzAJBgNVBAsMAmNj
 MRMwEQYDVQQDDAoxMC4xLjMuMTczMRQwEgYJKoZIhvcNAQkBFgVhZG1pbjCCASIw DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMKfpJ2BRoP4Uv6h
uliZw56HWBd/ uElqEqKPcZ5c4ieQQUdvFEOnMEeTJ655vA5zg1fg1N7kBNoUhwT3EHCD6/3Ml jlv FDVo78Bc2ZubXFIBLOTOt8bz4ZqAKmfugQ5EWFHe
OeNNq9KHYnJQd4kEjOb4DzEZ NokO47686FD9QGexwZrGfV1878TJmXu+6dGR38ta5NafWODufCXLCRLLQDTzMv2a SV7PC6TDjQdlTChssBSxVVj+0nyE
XMbFgMMCXJnapSmAwGoTiMaZGkFxR1xwDX6x R39rCuKFcuKkXLfR7scmKWCNwR4NgiXYoYxK6+wx1hTW2u+by0bqCuUq508CAwEA AaA8MDoGCSqGSIb3
DQEJDjEtMCswCQYDVR0TBAIwADALBgNVHQ8EBAMCBeAwEQYD VR0RBAowCIIGZXgzNjAwMA0GCSqGSIb3DQEBCwUAA4IBAQC7piG0tNssjzo8rP8x FAfc
1zKjOhR4jH8wfHFRUUo5TDQ/lg17YAdXHXFbWiERQyLcP4ubyK78DWIcAvcX vBjyqlG4vpJoNVCT/VJljv5XY2M3R82eMQHHMxDP+9U5wJvkkjyYDPFT2
oUMtgKp AsjTliCp9tYYQXJUBT+fmXJhkyPyJR8b6Edl6UHvJwSdLQnpvB8DNF2NrhUBJuh3 o2LDvOVvOh9nueXNc68Lscac3oyizFLkZmIJmNIIUcdAs
COf2iDb4yo/D2TJoemD r3he9ztURi+D2CpSqsOoo1wnKz3OgEE/+sYoT0aBFCaZ33ukvn2nmlyFSsgMqQB6 qZ3z -----END CERTIFICATE REQUEST
----- " before deletion
2024-06-06T07:35:48 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 6584: item 4: Certificate signing requ
est (CSR) Name test: Certificate signing request (CSR) unique ID was "73819f85d6fa6a22eaf9f3306f6ae8606449953b" before
 deletion
2024-06-06T07:35:48 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 6584: item 5: Certificate signing requ
est (CSR) Name test: Certificate signing request (CSR) unique name was "test" before deletion
2024-06-06T07:35:48 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 6584: item 6: Certificate signing requ
est (CSR) Name test: Certificate signing request (CSR) private key PEM string deleted
2024-06-06T07:35:48 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: Config change ID 6584: item 7: Certificate signing requ
est (CSR) Name test: Certificate signing request (CSR) private key is present was yes before deletion
2024-06-06T07:35:48 ex3600 mgmtd[7249]: [mgmtd.NOTICE]: AUDIT: (internal) Action ID 27307: requested by: (system) (ses
sion ID 487965)
```

```
2024-07-26T19:34:29 ex3600 mgmtd[7315]: [mgmtd.NOTICE]: AUDIT: Config change ID 28077: requested by: user ad
min (System Administrator) via CLI (session ID 2106561), 3 item(s) changed
2024-07-26T19:34:29 ex3600 mgmtd[7315]: [mgmtd.NOTICE]: AUDIT: Config change ID 28077: item 1: CMC RSA2 iden
tity 'test1' deleted
2024-07-26T19:34:29 ex3600 mgmtd[7315]: [mgmtd.NOTICE]: AUDIT: Config change ID 28077: item 2: CMC RSA2 iden
tity 'test1': private key deleted
2024-07-26T19:34:29 ex3600 mgmtd[7315]: [mgmtd.NOTICE]: AUDIT: Config change ID 28077: item 3: CMC RSA2 iden
tity 'test1': public key was "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCxuBeL243Q8qZ/XHzfENhXUU8X05xieb1g6mSMvT
3KQQfNiFkakZGyjWa18tsCrUaiqxqgff2HRp/m0xKrxp5WAN6/ykEaLhgE4bnwJFG1ITj3IyZ2Rsbv1nAMe6clZRIChEVv9+QApZNlE84uUI
Ui6yrd0UibJMrjyBJEag6DVD9g4/EwCc1yDuXETS2luYLB52JpXQwKjqfzfMXngFyq1zApxrNnvcslVIN9U6IkhsKEZiZEq4pfWzyV+4iIR5
3zXQeAu1ATtxRAlF+46rt0q4yAvJCYpYPDYo9iJ4ni0Er/dDFr+5nDmzo2xWvqpArYCoP6FXps1rL9QN4RkSRP  " before deletion
```

H. Changing of cryptographic keys

```
2024-07-25T11:14:56 ex3600 cli[545]: [cli.NOTICE]: AUDIT: user admin: Executing command: ssh serve
r host-key rsa2 public-key "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC2u7d0D3CK0f92t5kmNejlU1ayogvy+0
S3sM6dBkIdgRaRo/z+WyEjT+6TGYtulmn6e+mZPXaw0y7+6Kc2X8L5CnbHVM8T3ZpcW566uIQ/pJI6Pt1SU4zz3kIieWrJkHNn
gsKY/rgzj583DvmfXhnTQmFIDpK6t/iRprq6SKh8gV9Pns4w1BWeiqQ9YEM60F1RkERL+7yQBwOPOFGfxOVnDno2qs5TTMdtgr
QJ+kzfnXb9sQOF9LBMyRVcu92CvCf2qLC12JmBVRLcc7z0cnd81zfuxmoRE5ZHFgJITAZ82srN/wZwe0nHPdG66SxupeoHF8Sd
USUI61LHZVKSzU5vflTNEDjhyUNt3SEIn6hRIbG4H4tNOR0U/klyw85+MSY0mDmuvSW5q0/Q8iyw4EfWcJVoKmrB/9NSmW8URn
ebRdPWJ7B2wBHsC/eveoI6dbeMThbtH3Qb/KukbZrQOGyCKsdqVgdBvAlkKQqBbeMOjsHlBg0qduDxPH42YhH55js= root@tr
ellixvm2"
2024-07-25T11:14:56 ex3600 mgmtd[7315]: [mgmtd.NOTICE]: AUDIT: Config change ID 23550: requested b
y: user admin (System Administrator) via CLI (session ID 1753841), 1 item(s) changed
2024-07-25T11:14:56 ex3600 mgmtd[7315]: [mgmtd.NOTICE]: AUDIT: Config change ID 23550: item 1: SSH
 public RSA v2 host key changed from "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC2tqgei4BhvLFpnyKSZwtl
eG80N/k+L3JV1bHcjrl76DUsbgWwH+rLwnAn7o7AVoIwsg4UyTz+R0LbdYYkSRt0kuJxREd6FERhl2ONfTitkvR9AVzwgP23sa
ql3g6wNQ1yUK+/obkADYnufqmVN2cjowGx52O2LPAFQbmtw4wakXuLYWpWs2OmDT6042TxgyHxyvJ1OhB2d/Jb2xEz3YZMabfA
PidLPFGU/jSg2b6+rEK8ox2sI/dE0j+Lr8HoYg/wwsDoUEEcUL/ynxt0VG1MB2VxTuI0+LArpoqzw87EfUo1zdGVnA1w0J6IsM
zp92onkTMNKPKxSWAnSlahTob7  " to "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC2u7d0D3CK0f92t5kmNejlU1ay
ogvy+0S3sM6dBkIdgRaRo/z+WyEjT+6TGYtulmn6e+mZPXaw0y7+6Kc2X8L5CnbHVM8T3ZpcW566uIQ/pJI6Pt1SU4zz3kIieW
rJkHNngsKY/rgzj583DvmfXhnTQmFIDpK6t/iRprq6SKh8gV9Pns4w1BWeiqQ9YEM60F1RkERL+7yQBwOPOFGfxOVnDno2qs5T
TMdtgrQJ+kzfnXb9sQOF9LBMyRVcu92CvCf2qLC12JmBVRLcc7z0cnd81zfuxmoRE5ZHFgJITAZ82srN/wZwe0nHPdG66SxupE
oHF8SdUSUI61LHZVKSzU5vflTNEDjhyUNt3SEIn6hRIbG4H4tNOR0U/klyw85+MSY0mDmuvSW5q0/Q8iyw4EfWcJVoKmrB/9NS
mW8URnebRdPWJ7B2wBHsC/eveoI6dbeMThbtH3Qb/KukbZrQOGyCKsdqVgdBvAlkKQqBbeMOjsHlBg0qduDxPH42YhH55js= r
oot@trellixvm2"
```

I. Resetting passwords:

```
2023-09-14T09:12:02 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4795: item 1: local user account 'good' old password #1 deleted
2023-09-14T09:12:02 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4795: item 2: local user account 'good' old password #1: time set
 was 2023/05/29 18:20:51 before deletion
2023-09-14T09:12:02 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4795: item 3: local user account 'good' old password #2 added
2023-09-14T09:12:02 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4795: item 4: local user account 'good' old password #2: time set
 initially set to 2023/09/14 09:12:02
2023-09-14T09:12:02 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4795: item 5: local user account 'good': password changed from (u
ndisclosed password set) to (undisclosed password set)
```

J. Configuration of a new time server

```
2023-09-14T09:19:06 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4802: item 1: NTP server 10.1.4.67 added
2023-09-14T09:19:06 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4802: item 2: NTP server 10.1.4.67: initially set to enabled
2023-09-14T09:19:06 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4802: item 3: NTP server 10.1.4.67: NTP server keyid initially se
t to 0
2023-09-14T09:19:06 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4802: item 4: NTP server 10.1.4.67: prefer this server initially
set to disabled
2023-09-14T09:19:06 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4802: item 5: NTP server 10.1.4.67: NTP version initially set to
4
```

K. Failure to establish a HTTPS Session

```
2023-06-12T09:29:01 ex3600 httpd: AUDIT: httpd secure channel: SSL library error 1 in handshake with 10.1.3.175 (server localhost:443)
2023-06-12T09:29:01 ex3600 httpd: AUDIT: httpd secure channel: connection closed to 10.1.3.175 with abortive shutdown (server localhost
:443)
ex3600 #
```

L. Removal of configured time server

```
2023-09-14T09:18:00 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4801: item 1: NTP server 10.1.4.67 deleted
2023-09-14T09:18:00 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4801: item 2: NTP server 10.1.4.67: was enabled before deletion
2023-09-14T09:18:00 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4801: item 3: NTP server 10.1.4.67: NTP Server keyid was 13 befor
e deletion
2023-09-14T09:18:00 ex3600 mgmtd[18529]: [mgmtd.NOTICE]: AUDIT: Config change ID 4801: item 4: NTP server 10.1.4.67: prefer this server was disabl
ed before deletion
```

M. Failure to establish an SSH session

a. Authentication failure due to incorrect password and incorrect public key:

```
2023-11-09T12:05:54 ex3600 sshd[10233]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.1.3.
175  user=test
2023-11-09T12:05:54 ex3600 sshd[10233]: AUDIT: Authentication failure for user 'test' from host: 10.1.3.175 tty: unknown
2023-11-09T12:05:54 ex3600 sshd[10228]: error: PAM: Authentication failure for test from 10.1.3.175
2023-11-09T12:05:54 ex3600 sshd[10228]: User test failed to login via ssh2 from 10.1.3.175
2023-11-09T12:05:56 ex3600 sshd[10247]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.1.3.
175  user=test
2023-11-09T12:05:56 ex3600 sshd[10247]: AUDIT: Authentication failure for user 'test' from host: 10.1.3.175 tty: unknown
2023-11-09T12:05:56 ex3600 sshd[10228]: error: PAM: Authentication failure for test from 10.1.3.175
2023-11-09T12:05:56 ex3600 sshd[10228]: User test failed to login via ssh2 from 10.1.3.175
2023-11-09T12:05:58 ex3600 sshd[10295]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.1.3.
175  user=test
2023-11-09T12:05:58 ex3600 sshd[10295]: pam_tallybyname(sshd:auth): Too many login failures for user 'test': account now locked.
2023-11-09T12:05:58 ex3600 sshd[10295]: AUDIT: Authentication failure for user 'test' from host: 10.1.3.175 tty: unknown
2023-11-09T12:05:58 ex3600 sshd[10228]: error: PAM: Authentication failure for test from 10.1.3.175
2023-11-09T12:05:58 ex3600 sshd[10228]: User test failed to login via ssh2 from 10.1.3.175
2023-11-09T12:05:58 ex3600 sshd[10228]: ssh secure channel: Connection closed by 10.1.3.175 [preauth]
2023-11-09T12:05:58 ex3600 sshd[10228]: fatal: ssh secure channel: Connection closed by 10.1.3.175 port 59546 [preauth]
2023-11-09T12:05:58 ex3600 sshd[10228]: ssh secure channel: mm_request_receive: atomicio failed: Broken pipe
```

```
2023-09-18T09:41:21 ex3600 sshd[20116]: ssh secure channel: Session rekey request sent. [preauth]
2023-09-18T09:41:21 ex3600 sshd[20116]: ssh secure channel: Session rekey request received. [preauth]
2023-09-18T09:41:21 ex3600 sshd[20116]: ssh secure channel: client->server cipher: aes128-ctr, mac: hmac-sha2-512 [preauth]
2023-09-18T09:41:21 ex3600 sshd[20116]: ssh secure channel: server->client cipher: aes128-ctr, mac: hmac-sha2-512 [preauth]
2023-09-18T09:41:21 ex3600 sshd[20116]: ssh secure channel: kex: diffie-hellman-group14-sha1 [preauth]
2023-09-18T09:41:21 ex3600 sshd[20116]: ssh secure channel: Session rekey finished. [preauth]
2023-09-18T09:41:21 ex3600 sshd[20116]: ssh secure channel: SSH2 connection is established with 10.1.3.175 port 59026 [preauth]
2023-09-18T09:41:21 ex3600 sshd[20116]: User test failed to login via ssh2: RSA SHA256:ypdNaqxxrVN9Oyx6NXPfGt443zcioGlLin2p/ynJIaU from
 10.1.3.175
2023-09-18T09:41:23 ex3600 sshd[20122]: pam_ldap(sshd:account): No AAA Rules matched
2023-09-18T09:41:23 ex3600 sshd[20116]: SSH authentication: PAM
2023-09-18T09:41:23 ex3600 sshd[20116]: User test logged in via ssh2 from 10.1.3.175
2023-09-18T09:41:23 ex3600 cli[20127]: [cli.NOTICE]: user test: CLI launched
2023-09-18T09:41:23 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: User test (local user test) authentication method: local (password)
2023-09-18T09:41:23 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: User login: username 'test', role 'monitor', client 'CLI', line 'pts/1',
 remote address '10.1.3.175', auth method 'local', auth submethod 'password', session ID 991852
```

b. Cipher mismatch:

```
2023-09-08T08:41:26 ex3600 sshd[21590]: ssh secure channel: Session rekey request sent. [preauth]
2023-09-08T08:41:26 ex3600 sshd[21590]: ssh secure channel: Session rekey request received. [preauth]
2023-09-08T08:41:26 ex3600 sshd[21590]: fatal: ssh secure channel: Unable to negotiate with 10.1.3.175 port 58552: no matching cipher found. Their
 offer: aes128-cbc [preauth]
2023-09-08T08:41:26 ex3600 sshd[21590]: ssh secure channel: mm_request_receive: atomicio failed: Broken pipe

ex3600 #
```

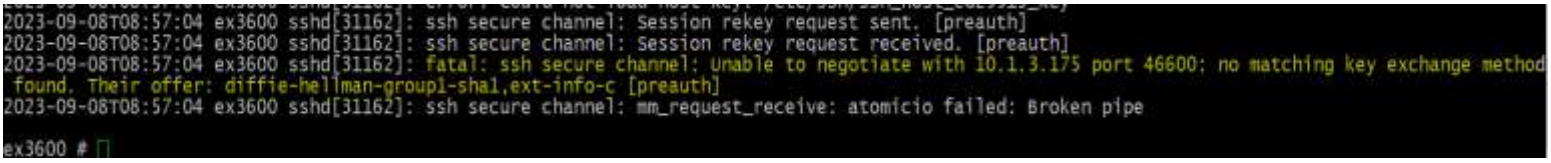
c. Host key algorithm mismatch:

```
2023-09-08T08:46:47 ex3600 sshd[5123]: ssh secure channel: Session rekey request sent. [preauth]
2023-09-08T08:46:47 ex3600 sshd[5123]: ssh secure channel: Session rekey request received. [preauth]
2023-09-08T08:46:47 ex3600 sshd[5123]: fatal: ssh secure channel: Unable to negotiate with 10.1.3.175 port 33466: no matching host key type found.
 Their offer: ssh-dss [preauth]
2023-09-08T08:46:47 ex3600 sshd[5123]: ssh secure channel: mm_request_receive: atomicio failed: Broken pipe

ex3600 #
```

d. HMAC algorithm mismatch:

e. Key exchange algorithm mismatch:



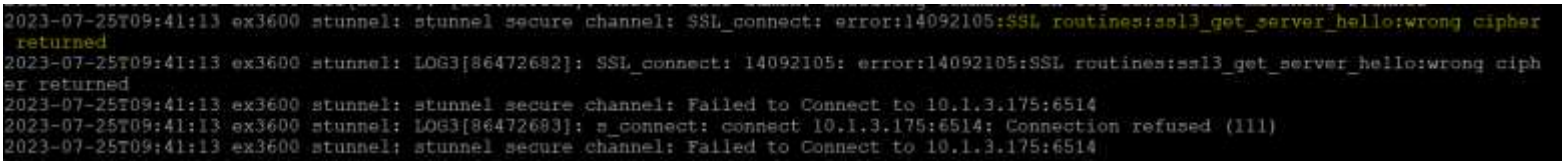
N. Failure to establish a TLSC Session

a. Unsupported certificate purpose:

b. Wrong certificate type:

c. Unsupported algorithm:

d. Unsupported ciphersuite:



e. Unsupported curve:

f. Unsupported TLS version:

g. Bad signature:

h. Digest check failed:

i. Failure due to data received between ChangeCipherSpec (CCS) message and finished:

j. Modified byte in server's nonce in the Server Hello handshake message:

```
2024-07-18T08:38:52 ex3600 stunnel: stunnel secure channel: opened, connected to 10.1.5.162:6514 (from lo
cal interface address 10.1.3.173:52414)
2024-07-18T08:38:52 ex3600 stunnel: stunnel secure channel: error queue: error:1408D07B:SSL routines:ssl3
_get_key_exchange:bad signature
2024-07-18T08:38:52 ex3600 stunnel: LOG3[169604]: error queue: 1408D07B: error:1408D07B:SSL routines:ssl3
_get_key_exchange:bad signature
2024-07-18T08:38:52 ex3600 stunnel: stunnel secure channel: SSL_connect: error:04097068:rsa routines:RSA_
private_encrypt:bad signature
2024-07-18T08:38:52 ex3600 stunnel: LOG3[169604]: SSL_connect: 4097068: error:04097068:rsa routines:RSA_p
rivate_encrypt:bad signature
2024-07-18T08:38:52 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.5.162:6514
```

k. Certificate verification failure due to invalid CN and no SAN:

```
2023-07-26T08:46:22 ex3600 stunnel: LOG4[67332325]: CERT: No matching IP address found
2023-07-26T08:46:22 ex3600 stunnel: LOG4[67332325]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=10.1.3.170
2023-07-26T08:46:22 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certif
icate verify failed
2023-07-26T08:46:22 ex3600 stunnel: LOG3[67332325]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:cert
ificate verify failed
2023-07-26T08:46:22 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
```

```
2023-07-26T10:58:29 ex3600 stunnel: LOG4[2611582]: CERT: No matching host name found
2023-07-26T10:58:29 ex3600 stunnel: LOG4[2611582]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=invalid.acumensec.local
2023-07-26T10:58:29 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certif
icate verify failed
2023-07-26T10:58:29 ex3600 stunnel: LOG3[2611582]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:certi
ficate verify failed
```

l. Certificate verification failure due to invalid SAN:

```
2023-07-26T09:08:37 ex3600 stunnel: LOG4[68360636]: CERT: No matching IP address found
2023-07-26T09:08:37 ex3600 stunnel: LOG4[68360636]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=10.1.3.175
2023-07-26T09:08:37 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certif
icate verify failed
2023-07-26T09:08:37 ex3600 stunnel: LOG3[68360636]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:cert
ificate verify failed
2023-07-26T09:08:37 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
```

```
2023-07-26T11:14:59 ex3600 stunnel: LOG4[3693557]: CERT: No matching host name found
2023-07-26T11:14:59 ex3600 stunnel: LOG4[3693557]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=trellixvm2.acumensec.local
2023-07-26T11:14:59 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certif
icate verify failed
2023-07-26T11:14:59 ex3600 stunnel: LOG3[3693557]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:certi
ficate verify failed
2023-07-26T11:14:59 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
```

m. Certificate verification failure due to pre-verification error:

```
2023-07-25T13:10:59 ex3600 stunnel: LOG4[124734]: CERT: Pre-verification error: unable to get local issuer certificate
2023-07-25T13:10:59 ex3600 stunnel: LOG4[124734]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=10.1.3.175
2023-07-25T13:10:59 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:10:59 ex3600 stunnel: LOG3[124734]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:10:59 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
2023-07-25T13:10:59 ex3600 stunnel: LOG4[124735]: CERT: Pre-verification error: unable to get local issuer certificate
2023-07-25T13:10:59 ex3600 stunnel: LOG4[124735]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=10.1.3.175
2023-07-25T13:10:59 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:10:59 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
```

n. Expired certificate:

```
2023-07-25T13:27:02 ex3600 stunnel: LOG4[575997]: CERT: Pre-verification error: certificate has expired
2023-07-25T13:27:02 ex3600 stunnel: LOG4[575997]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=10.1.3.175
2023-07-25T13:27:02 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:27:02 ex3600 stunnel: LOG3[575997]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:27:02 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
2023-07-25T13:27:02 ex3600 stunnel: LOG4[575998]: CERT: Pre-verification error: certificate has expired
2023-07-25T13:27:02 ex3600 stunnel: LOG4[575998]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=10.1.3.175
2023-07-25T13:27:02 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:27:02 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
```

O. Failure to establish a TLSS Session

```
2023-06-12T09:12:39 ex3600 httpd: AUDIT: httpd secure channel: SSL library error 1 in handshake with 10.1.3.175 (server localhost:443)
2023-06-12T09:12:39 ex3600 httpd: AUDIT: httpd secure channel: connection closed to 10.1.3.175 with abortive shutdown (server localhost
:443)
```

P. Unsuccessful login attempts limit is met or exceeded.

```
2023-05-29T17:45:01 ex3600 sshd[25039]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.1.3.
175  user=test
2023-05-29T17:45:01 ex3600 sshd[25039]: AUDIT: Authentication failure for user 'test' from host: 10.1.3.175 tty: unknown
2023-05-29T17:45:01 ex3600 sshd[25034]: error: PAM: Authentication failure for test from 10.1.3.175
2023-05-29T17:45:01 ex3600 sshd[25034]: User test failed to login via ssh2 from 10.1.3.175
2023-05-29T17:45:03 ex3600 sshd[26187]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.1.3.
175  user=test
2023-05-29T17:45:03 ex3600 sshd[26187]: AUDIT: Authentication failure for user 'test' from host: 10.1.3.175 tty: unknown
2023-05-29T17:45:03 ex3600 sshd[25034]: error: PAM: Authentication failure for test from 10.1.3.175
2023-05-29T17:45:03 ex3600 sshd[25034]: User test failed to login via ssh2 from 10.1.3.175
2023-05-29T17:45:06 ex3600 sshd[27311]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.1.3.
175  user=test
2023-05-29T17:45:06 ex3600 sshd[27311]: pam_tallybyname(sshd:auth): Too many login failures for user 'test': account now locked.
2023-05-29T17:45:07 ex3600 sshd[27311]: AUDIT: Authentication failure for user 'test' from host: 10.1.3.175 tty: unknown
2023-05-29T17:45:07 ex3600 sshd[25034]: error: PAM: Authentication failure for test from 10.1.3.175
2023-05-29T17:45:07 ex3600 sshd[25034]: User test failed to login via ssh2 from 10.1.3.175
```

```
2023-05-19T16:07:59 ex3600 httpd: message repeated 3 times: [ AUDIT: httpd secure channel: connection closed to 192.168.254.169 with st
andard shutdown (server localhost:443)]
2023-05-19T16:08:00 ex3600 wsmd[15605]: AUDIT: Authentication failure for user 'test' from host: 192.168.254.169 tty: unknown
2023-05-19T16:08:01 ex3600 su: AUDIT: (to postgres) admin on none
2023-05-19T16:08:01 ex3600 su: AUDIT: (to postgres) admin on none
2023-05-19T16:08:01 ex3600 su: AUDIT: (to postgres) admin on none
2023-05-19T16:08:06 ex3600 httpd: AUDIT: httpd secure channel: SSL connection is established with 192.168.254.169 using cipher suite EC
DHE-RSA-AES128-GCM-SHA256.
2023-05-19T16:08:06 ex3600 httpd: message repeated 3 times: [ AUDIT: httpd secure channel: SSL connection is established with 192.168.2
54.169 using cipher suite ECDHE-RSA-AES128-GCM-SHA256.]
2023-05-19T16:08:10 ex3600 wsmd[15605]: AUDIT: Authentication failure for user 'test' from host: 192.168.254.169 tty: unknown
2023-05-19T16:08:17 ex3600 wsmd[15605]: AUDIT: Authentication failure for user 'test' from host: 192.168.254.169 tty: unknown
2023-05-19T16:08:21 ex3600 httpd: AUDIT: httpd secure channel: connection closed to 192.168.254.169 with standard shutdown (server loca
lhost:443)
2023-05-19T16:08:21 ex3600 httpd: message repeated 2 times: [ AUDIT: httpd secure channel: connection closed to 192.168.254.169 with st
andard shutdown (server localhost:443)]
2023-05-19T16:08:24 ex3600 wsmd[15605]: AUDIT: Denying access to user 'test': Maximum number of failed logins reached, account locked.
 You may try again in 113 second(s).
2023-05-19T16:08:24 ex3600 wsmd[15605]: AUDIT: Authentication failure for user 'test' from host: 192.168.254.169 tty: unknown
2023-05-19T16:08:26 ex3600 httpd: AUDIT: httpd secure channel: connection closed to 192.168.254.169 with standard shutdown (server loca
lhost:443)
2023-05-19T16:08:28 ex3600 httpd: AUDIT: httpd secure channel: SSL connection is established with 192.168.254.169 using cipher suite EC
DHE-RSA-AES128-GCM-SHA256.
2023-05-19T16:08:33 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: (internal) Action ID 24373: requested by: (system) (session ID 192)
2023-05-19T16:08:33 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: (internal) Action ID 24373: descr: Check for maxmind db update immediate
ly.
2023-05-19T16:08:33 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: (internal) Action ID 24373: status: completed with success
2023-05-19T16:08:37 ex3600 wsmd[15605]: AUDIT: Denying access to user 'test': Maximum number of failed logins reached, account locked.
 You may try again in 100 second(s).
2023-05-19T16:08:37 ex3600 wsmd[15605]: AUDIT: Authentication failure for user 'test' from host: 192.168.254.169 tty: unknown
2023-05-19T16:08:48 ex3600 httpd: AUDIT: httpd secure channel: connection closed to 192.168.254.169 with standard shutdown (server loca
lhost:443)
2023-05-19T16:08:52 ex3600 httpd: AUDIT: httpd secure channel: connection closed to 192.168.254.169 with standard shutdown (server loca
lhost:443)
```

Q. All use of identification and authentication mechanism.

a. Successful and unsuccessful authentication of Web UI:

```
2023-05-30T11:30:43 ex3600 wsmd[15605]: [wsmd.NOTICE]: User admin (System Administrator) logged into Web UI from 192.168.228.38
2023-05-30T11:30:43 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: User admin (local user admin) authentication method: local (password)
2023-05-30T11:30:43 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: User login: username 'admin', full name 'System Administrator', role 'ad
min', client 'Web', line 'web/8', remote address '192.168.228.38', auth method 'local', auth submethod 'password', session ID 1501676
2023-05-30T11:30:45 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 160437: requested by: user admin (System Administrator) via We
b UI (session ID 1501676)
2023-05-30T11:30:45 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 160437: descr: Query redis for failed service status
2023-05-30T11:30:45 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 160437: status: completed with success
2023-05-30T11:30:45 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 160438: requested by: user admin (System Administrator) via We
b UI (session ID 1501676)
2023-05-30T11:30:45 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 160438: descr: End of life status of the appliance
2023-05-30T11:30:45 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 160438: status: completed with success
```

```
2023-05-30T11:30:16 ex3600 wsmd[15605]: pam_unix(wsmd:auth): authentication failure; logname= uid=0 euid=0 tty= ruser= rhost=192.168.22
8.38  user=admin
2023-05-30T11:30:16 ex3600 wsmd[15605]: AUDIT: Authentication failure for user 'admin' from host: 192.168.228.38 tty: unknown
2023-05-30T11:30:16 ex3600 wsmd[15605]: [wsmd.NOTICE]: Authentication failure for user admin from 192.168.228.38
2023-05-30T11:30:16 ex3600 webui[15873]: tid 15883: [webui.ERR]: [184] [unknown] [unknown] Mdc Login failure Incorrect user id or passw
ord.
2023-05-30T11:30:17 ex3600 httpd: AUDIT: httpd secure channel: connection closed to 192.168.228.38 with standard shutdown (server local
host:443)
2023-05-30T11:30:17 ex3600 httpd: message repeated 4 times: [ AUDIT: httpd secure channel: connection closed to 192.168.228.38 with sta
ndard shutdown (server localhost:443)]
```

b. Successful and unsuccessful authentication of Remote CLI:

```
2023-05-30T11:42:54 ex3600 sshd[14046]: User admin (System Administrator) logged in via ssh2 from 10.1.3.175
2023-05-30T11:42:54 ex3600 cli[14054]: [cli.NOTICE]: user admin: CLI launched
2023-05-30T11:42:54 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: User admin (local user admin) authentication method: local (password)
2023-05-30T11:42:54 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: User login: username 'admin', full name 'System Administrator', role 'ad
min', client 'CLI', line 'pts/2', remote address '10.1.3.175', auth method 'local', auth submethod 'password', session ID 1502640
```

```
2023-05-30T11:39:22 ex3600 sshd[16133]: User admin (System Administrator) failed to login via ssh2: RSA 51:ba:b7:96:ee:12:3c:0d:84:0b:d
4:d7:c1:92:06:e1:62:ee:c4:b5 from 10.1.3.175
2023-05-30T11:39:25 ex3600 sshd[16138]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.1.3.
175  user=admin
2023-05-30T11:39:25 ex3600 sshd[16138]: AUDIT: Authentication failure for user 'admin' from host: 10.1.3.175 tty: unknown
2023-05-30T11:39:25 ex3600 sshd[16133]: error: PAM: Authentication failure for admin from 10.1.3.175
2023-05-30T11:39:25 ex3600 sshd[16133]: User admin (System Administrator) failed to login via ssh2 from 10.1.3.175
```

c. Successful and unsuccessful authentication of Console:

```
2023-06-26T12:59:14 ex3600 mgmtd[7298]: [mgmtd.NOTICE]: AUDIT: User login: username 'admin', full name 'System Administrator', role 'ad
min', client 'CLI', line 'tty1', remote hostname '(local device)', auth method 'local', auth submethod 'password', session ID 16911
2023-06-26T12:59:14 ex3600 cli[11341]: [cli.NOTICE]: AUDIT: user admin: Logged in with session ID 16911
2023-06-26T12:59:38 ex3600 mgmtd[7298]: [mgmtd.NOTICE]: AUDIT: (internal) Action ID 980: requested by: (system) (session ID 16936)
```

```
2023-06-26T12:57:36 ex3600 login: AUDIT: Authentication failure for user 'admin' from host: none tty: tty1
2023-06-26T12:57:47 ex3600 mgmtd[7298]: [mgmtd.NOTICE]: AUDIT: (internal) Action ID 977: requested by: (system) (session ID 318)
```

R. Unsuccessful attempt to validate the certificate

a. Certificate verification failure due to invalid/incomplete certificate chain:

```
2023-07-25T13:10:59 ex3600 stunnel: LOG4[124734]: CERT: Pre-verification error: unable to get local issuer certificate
2023-07-25T13:10:59 ex3600 stunnel: LOG4[124734]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=10.1.3.175
2023-07-25T13:10:59 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:10:59 ex3600 stunnel: LOG3[124734]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:10:59 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
2023-07-25T13:10:59 ex3600 stunnel: LOG4[124735]: CERT: Pre-verification error: unable to get local issuer certificate
2023-07-25T13:10:59 ex3600 stunnel: LOG4[124735]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=10.1.3.175
2023-07-25T13:10:59 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:10:59 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
```

b. Expired server certificate:

```
2023-07-25T13:27:02 ex3600 stunnel: LOG4[575997]: CERT: Pre-verification error: certificate has expired
2023-07-25T13:27:02 ex3600 stunnel: LOG4[575997]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=10.1.3.175
2023-07-25T13:27:02 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:27:02 ex3600 stunnel: LOG3[575997]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:27:02 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
2023-07-25T13:27:02 ex3600 stunnel: LOG4[575998]: CERT: Pre-verification error: certificate has expired
2023-07-25T13:27:02 ex3600 stunnel: LOG4[575998]: Rejected by CERT at depth=0: C=US, O=acumen, OU=cc, CN=10.1.3.175
2023-07-25T13:27:02 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verif
y failed
2023-07-25T13:27:02 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
```

c. Revoked server certificate:

```
2023-08-10T13:27:27 ex3600 stunnel: LOG3[4835510]: OCSP: Certificate revoked
2023-08-10T13:27:27 ex3600 stunnel: LOG4[4835510]: Rejected by OCSP at depth=0: C=US, O=acumensec, OU=CC, CN=10.1.3.175
2023-08-10T13:27:27 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certif
icate verify failed
2023-08-10T13:27:27 ex3600 stunnel: LOG3[4835510]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:certi
ficate verify failed
2023-08-10T13:27:27 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
```

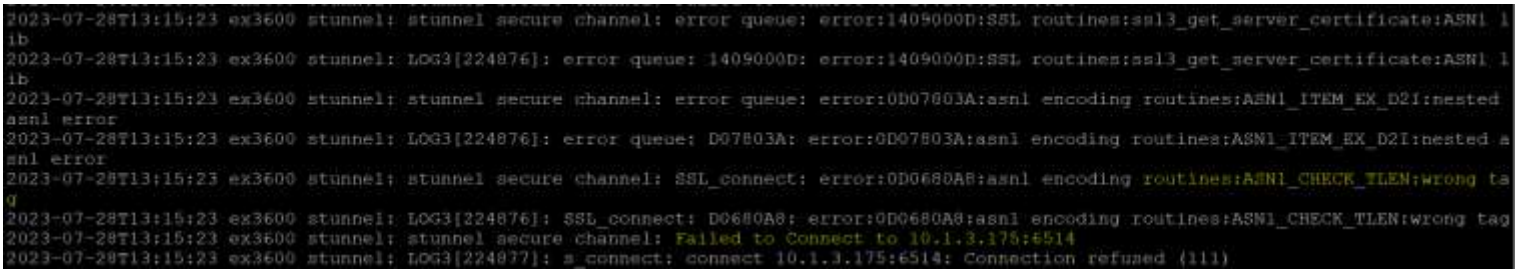
d. Revoked Intermediate CA Certificate:

```
2023-08-10T13:47:53 ex3600 stunnel: LOG3[6033580]: OCSP: Certificate revoked
2023-08-10T13:47:53 ex3600 stunnel: LOG4[6033580]: Rejected by OCSP at depth=1: C=US, O=acumensec, OU=CC, CN=OCSP-ICA
2023-08-10T13:47:53 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certif
icate verify failed
2023-08-10T13:47:53 ex3600 stunnel: LOG3[6033580]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:certi
ficate verify failed
2023-08-10T13:47:53 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
```

e. Invalid OCSP signer certificate:

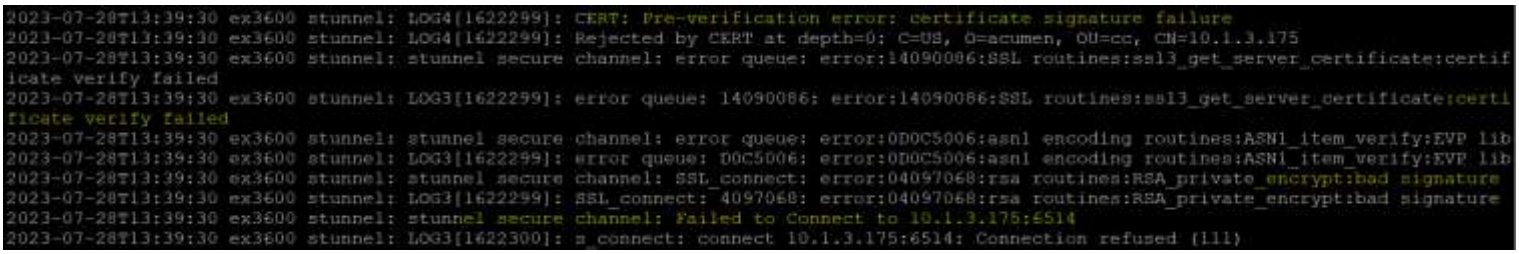
```
2023-11-13T14:17:45 ex3600 stunnel: stunnel secure channel: opened, connected to 10.1.3.175:6514 (from local interface address 10.1.3.1
73:55514)
2023-11-13T14:17:45 ex3600 stunnel: stunnel secure channel: error queue: error:27069070:OCSP routines:OCSP_basic_verify:root ca not tru
sted
2023-11-13T14:17:45 ex3600 stunnel: LOG3[0]: error queue: 27069070: error:27069070:OCSP routines:OCSP_basic_verify:root ca not trusted
2023-11-13T14:17:45 ex3600 stunnel: stunnel secure channel: OCSP: OCSP_basic_verify: error:2706A067:OCSP routines:OCSP_CHECK_DELEGATED:
missing ocspsigning usage
2023-11-13T14:17:45 ex3600 stunnel: LOG3[0]: OCSP: OCSP_basic_verify: 2706A067: error:2706A067:OCSP routines:OCSP_CHECK_DELEGATED:missi
ng ocspsigning usage
2023-11-13T14:17:45 ex3600 stunnel: LOG4[0]: Rejected by OCSP at depth=0: C=US, O=acumensec, OU=CC, CN=10.1.3.175
2023-11-13T14:17:45 ex3600 stunnel: stunnel secure channel: SSL_connect: error:14090086:SSL routines:ssl3_get_server_certificate:certif
icate verify failed
2023-11-13T14:17:45 ex3600 stunnel: LOG3[0]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:certificate
 verify failed
2023-11-13T14:17:45 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
```

f. Error due to modified certificate bytes:



g. Failure due to modified byte in signature:

h. Failure due to modified byte in the public key:



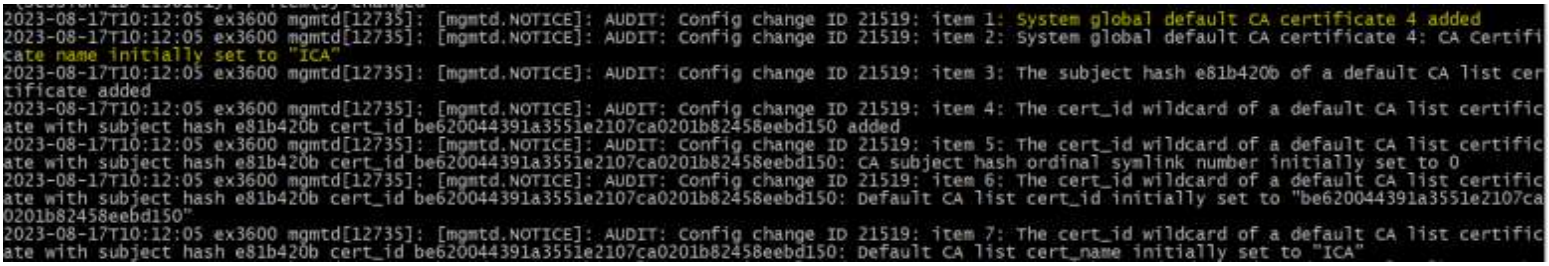
i. Error due to modified public key:

j. Basic constraint is not present in the CA certificate:

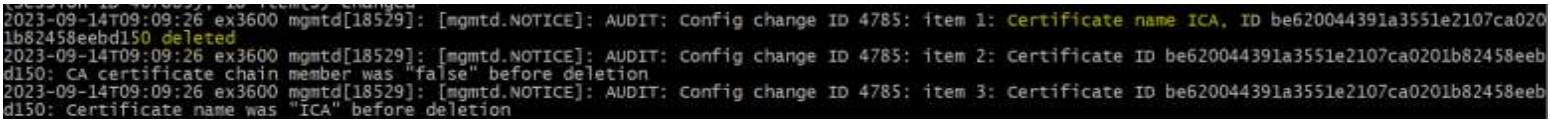
k. Basic constraint is set to false in the CA certificate:

l. Certificate verification failure due to OCSP responder issue:

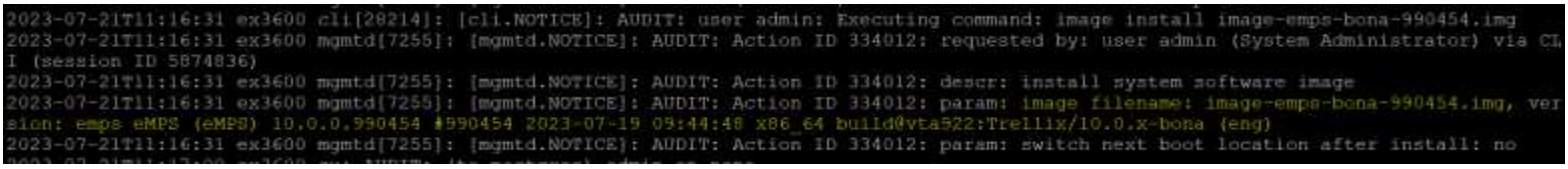
m. Addition of certificate**:**



n. Removal of certificate**:**

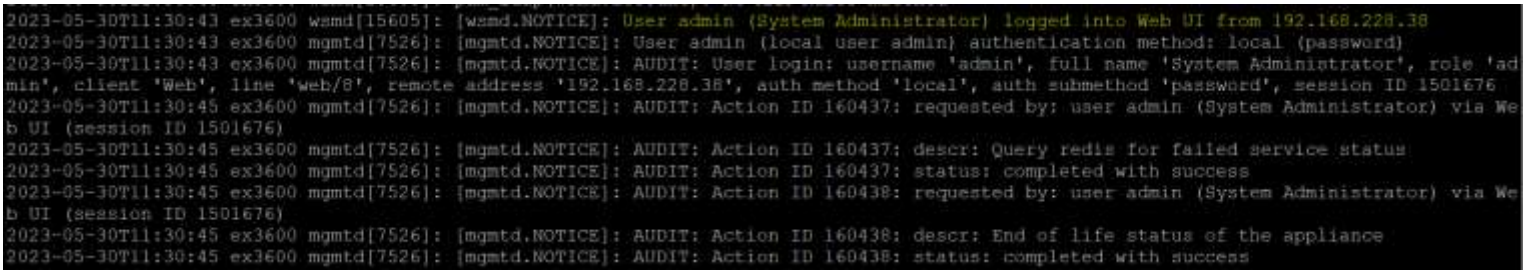


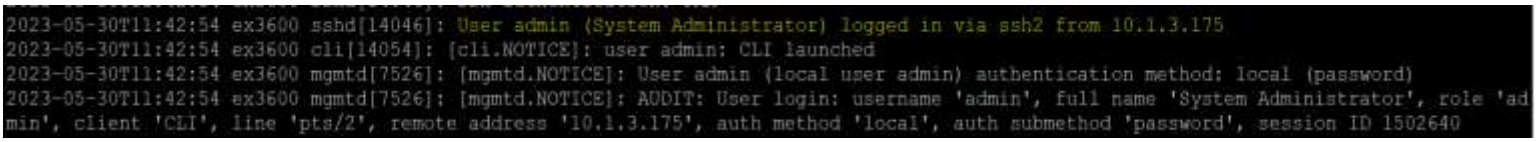
S. Any attempt to initiate a manual update



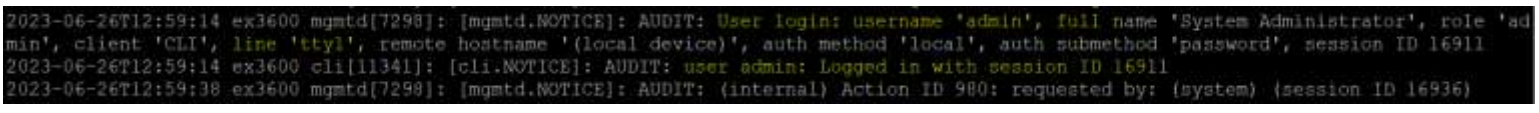
T. All management activities of TSF data

a. Ability to administer the TOE remotely:

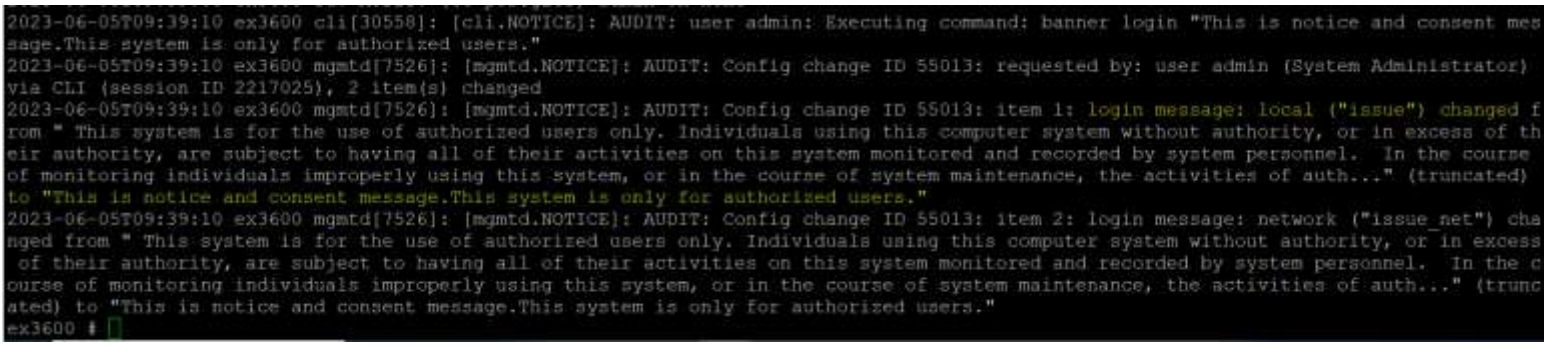




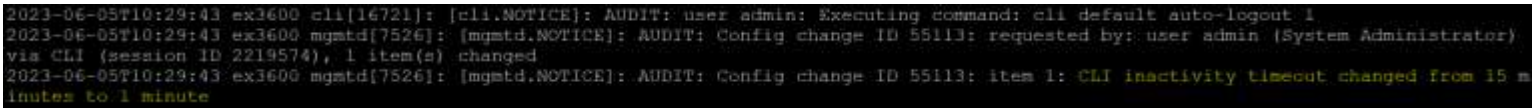
b. Ability to administer the TOE locally:

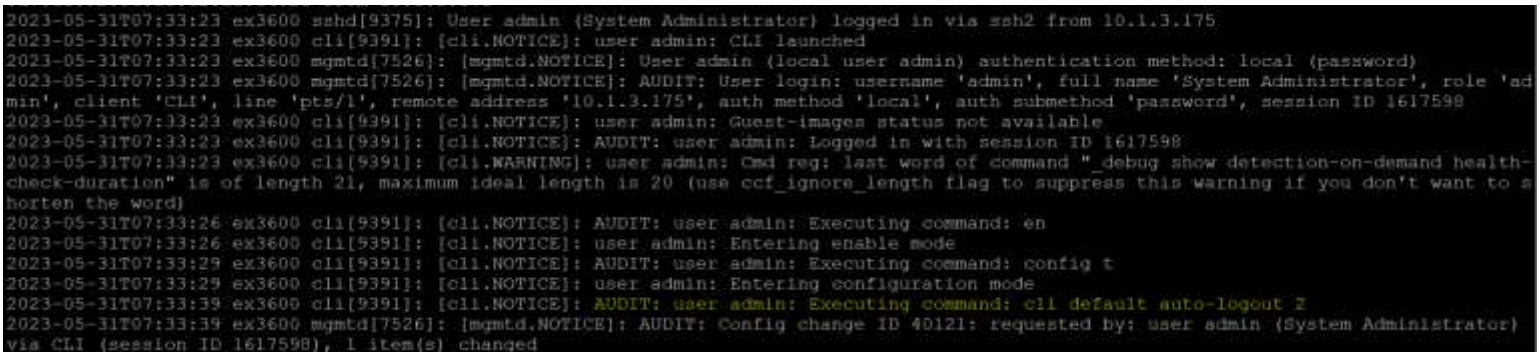


c. Ability to configure the access banner:



d. Ability to configure the session inactivity time before session termination or locking:





e. Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates:

f. Ability to configure the authentication failure parameters for FIA_AFL.1:

```
2023-05-19T15:31:51 ex3600 cli[29005]: [cli.NOTICE]: AUDIT: user admin: Executing command: aaa authentication attempts lockout max-fail
 3
2023-05-19T15:31:51 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Config change ID 5537: requested by: user admin (System Administrator) v
ia CLI (session ID 217575), 1 item(s) changed
2023-05-19T15:31:51 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Config change ID 5537: item 1: Authentication failure lockouts: number o
f consecutive failures required for lockout changed from 4 to 3
2023-05-19T15:31:58 ex3600 cli[29005]: [cli.NOTICE]: AUDIT: user admin: Executing command: aaa authentication attempts lockout unlock-t
ime 120
2023-05-19T15:31:58 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Config change ID 5538: requested by: user admin (System Administrator) v
ia CLI (session ID 217575), 1 item(s) changed
2023-05-19T15:31:58 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Config change ID 5538: item 1: Authentication failure lockouts: unlock t
ime (time since last failure until a locked-out account will permit another login attempt) changed from 60 seconds to 120 seconds
```

g. Ability to configure audit behaviour:

```
2024-07-25T10:50:46 ex3600 cli[6963]: [cli.NOTICE]: AUDIT: user admin: Executing command: logging
files rotation criteria size 2
2024-07-25T10:50:46 ex3600 mgmtd[7315]: [mgmtd.NOTICE]: AUDIT: Config change ID 23496: requested b
y: user admin (System Administrator) via CLI (session ID 1749344), 1 item(s) changed
2024-07-25T10:50:46 ex3600 mgmtd[7315]: [mgmtd.NOTICE]: AUDIT: Config change ID 23496: item 1: log
ging: maximum size of log file before rotation (absolute) changed from 1048576 bytes to 2097152 by
tes
```

```
2023-05-31T07:15:14 ex3600 cli[32730]: [cli.NOTICE]: AUDIT: user admin: Executing command: logging files rotation max-num 5
2023-05-31T07:15:26 ex3600 cli[32730]: [cli.NOTICE]: AUDIT: user admin: Executing command: exit
2023-05-31T07:15:26 ex3600 cli[32730]: [cli.NOTICE]: user admin: Leaving configuration mode
ex3600 #
```

h. Ability to modify the behaviour of the transmission of audit data to an external IT entity:

```
2023-09-18T06:50:29 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 9979: item 1: syslog: remote sink 10.1.3.175 added
2023-09-18T06:50:29 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 9979: item 2: syslog: remote sink 10.1.3.175: minimum l
og severity initially set to "notice"
2023-09-18T06:50:29 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 9979: item 3: syslog: remote sink 10.1.3.175: per-facil
ity override initially set to enabled
2023-09-18T06:50:29 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 9979: item 4: syslog: remote sink 10.1.3.175: server po
rt initially set to 6514
2023-09-18T06:50:29 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 9979: item 5: syslog: remote sink 10.1.3.175: transport
 protocol initially set to "tls"
```

i. Ability to configure the cryptographic functionality

```
2024-07-26T17:51:37 ex3600 mgmtd[7315]: [mgmtd.INFO]: ssh server rsa2 private hostkey key length =
 2048 bits
2024-07-26T17:51:37 ex3600 mgmtd[7315]: [mgmtd.INFO]: ssh server rsa2 public hostkey key length =
2048 bits
2024-07-26T17:51:37 ex3600 mgmtd[7315]: [mgmtd.NOTICE]: AUDIT: Config change ID 27833: item 1: SSH
 private RSA v2 host key changed
2024-07-26T17:51:37 ex3600 mgmtd[7315]: [mgmtd.NOTICE]: AUDIT: Config change ID 27833: item 2: SSH
 public RSA v2 host key changed from "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCuk7QCdXzfhCN0pQeNxeT2
g1TUfFF9bQi26caemiJzvKA0/qpiBRmdYTkvTxUxkFc3u1ZbHIV2Xjpit0RFZDE8KI0e8leRW09tWr/RMUjX9ehHdin1tXZTXh
Xl5ReGl3e5viGUz9IauF034eBWxU+M2V2JoZsTNldHWr+Xx29wiuz3B6wDR++7KRXH23n3t4KP6cO6Uuo5j3FPpBu93Hnv02JD
rYy/WEsd7rIG2m6f+OCb40pwCrkhaK70eNHyYYPmOzhc9jWVe6fPL2f2SiHCd1uTE2T2+V/AvcTdWDd1VMOnzh19TsLESPNAvb
P4LRo+uND4dC/LNjcbX2l8TJdh  " to "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDJPAgJTvXnn4IqQwmtJbCyPErK
Lx427XtzMoRLgykWdxoGlc98KNhBN0GpWjMsBxJITW3rC+dDwdvacFxODwFKM+HWQnAjNEC7hJCRmygK4S2MCsVy/kcCAcmsOX
nR+td6jmWs35/b5vq4fzk2K3YE0v4OoPoLyosru85hq0qLDA23qcDLWX6pYXgQy8FrEcBOC0D6TmeXrcnx2Bd8fH1Wx7GbYPOz
TlWPegs9taX1jvwvDsRZHbqC0fmkpHxvoGWeg4K5DNGP33zYcJRKYBvgoijU+1j85ooE6tqdP1K92U0v+DccdXdO/Dr3D088Lk
7iDpzIpw9Myk4ho95FVWCx  "
```

j. Ability to manage the cryptographic keys:

```
2023-07-31T12:46:26 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Action ID 277605: descr: Generate certificate signing request (CSR)
2023-07-31T12:46:26 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Action ID 277605: param: CSR name: "Test"
2023-07-31T12:46:26 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Action ID 277605: param: common name (hostname or contact name): ""
2023-07-31T12:46:26 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Action ID 277605: param: CSR key type: "rsa"
2023-07-31T12:46:26 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Action ID 277605: param: overwrite: no
2023-07-31T12:46:26 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Action ID 277605: param: Subject Alternative Name DNS list: ""
2023-07-31T12:46:26 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Action ID 277605: param: Subject Alternative Name IP address list: ""
2023-07-31T12:46:26 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Action ID 277605: param: Subject Alternative Name URI list: ""
2023-07-31T12:46:26 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Action ID 277605: param: Subject Alternative Name email address list: "
"
2023-07-31T12:46:27 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Config change ID 26574: requested by: user admin (System Administrator)
 via CLI (session ID 2647234), 7 item(s) changed
2023-07-31T12:46:27 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Config change ID 26574: item 1: Certificate signing request (CSR) Name
Test added
2023-07-31T12:46:27 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Config change ID 26574: item 2: Certificate signing request (CSR) Name
Test: Certificate signing request comment initially set to ""
2023-07-31T12:46:27 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Config change ID 26574: item 3: Certificate signing request (CSR) Name
Test: Certificate signing request (CSR) PEM string initially set to "-----BEGIN CERTIFICATE REQUEST----- MIIEFDCCAnwCAQAwgZIxCzAJBgNVBA
YTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlh MREwDwYDVQQHDAhTYW4gSm9zZTEQMA4GA1UECgwHVHJlbGxpeDE1MCAGA1UECwwZ VHJlbGxpeCBTZWN1cml0eSBQbGF0Zm9ybTE
PMA0GA1UEAwwGZXgzNjAwMRQwEgYJ KoZIhvcNAQkBFgVhZGlpbjCCAaIwDQYJKoZIhvcNAQEBBQADggGPADCCAYoCggGB AMEeExrwGlOdjzRmJFBpHC2nLx/NyxF8GlVsAHkV
BV+8BhIAoPTKc5tjFkCmv8Z2 1ZlmTqCOx5Mi5w1AKVxw4yulyQC3GFBzNkRYMhCjdzT5wT4fRuEyuy3YXxv6WoWM V1N1GoycD0/SjrngncCBUHYwHHSfQYJutZPNzhQz6K/tj
t9r2/KLi6DJZyzjHxbv LYZLZUxcD+BrnWiu8EEP9CuRlDMmSX1ZivWNUW8hmmJxuynNwLJ3VJXgKQTTAFYt N)PWVoyO1NbpEMhkBUMm97R1psz+Ttd8hCM9HnUTbu+wXhcCYS
zBB7lnuttpBUi6 wXDNcHygkdbgjqcLDfwJSNM5Kw2g705LOjNoZkyFqM60q7Oq2siKWOpMdDPyvrfW R4EAWia1Gi93epwmy+0IL837a/76DAKePiKy95vavjQ2uZP953cQVbt
385OIkHiP yiVGt2He83TlyvopdF3knfApmKiBDX55hL/9O/T03bMNiqSzgFS2vEHlm5440qc8 wwIDAQABoDwwOgYJKoZIhvcNAQkOMS0wKzAJBgNVHRMEAjAAMAsGA1UdDwQE
AwIF 4DARBgNVHREECjAIggZleDM2MDAwDQYJKoZIhvcNAQELBQADggGBAC8ac60ci2V9 qAlF+DkBCLkxJT8bEhioTvqQ5R64aCQJc+klwyQ6gutTyTke+b/ou8oH/iVn8HDd
zzFTiKgvdTNI9JOXiPwFG5gUnZJkm3iA+p0LGfmsw4aUcwgIqhJroBPISHC+Nujn zmh9c9TxjlgJeywlNrzH0Tb0Sa9M5Ig8L4FIOP9CaK1Z+sljZmMaQLIYY65WjvQU UazxW
Ge9o0ORIb7JpyQVO4EaAc7cWVF8LHFAwvLzBAniyo9XdB/925LxDRSjolLY QyT6GKa9KxbZhn0VY3mPJagwz3w+77Yr8sSnAVn8+Fk+DHzfXhOtnznmTRHylMlY 0rgXVBSHc4
BF5kx9WYSWAmVqGpN2n2W0fkuk7Oml4meb2XriSsar/qhfieeh/NcZ Z+wjJxDJcoKplAYValyaNcqfgUa9Xq4/QwyLfAHLU+HsetaM3f8ZVZmGvYbLwjU0 bOOEYioiBS/y/iP
UHNuwWNspCT1yl4wfvMFtHvbwCr1uDLBP7g9+0w== -----END CERTIFICATE REQUEST----- "
2023-07-31T12:46:27 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Config change ID 26574: item 4: Certificate signing request (CSR) Name
Test: Certificate signing request (CSR) unique ID initially set to "85e563dleb9f2eda9f39ba0f25394de3b2a41332"
2023-07-31T12:46:27 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Config change ID 26574: item 5: Certificate signing request (CSR) Name
Test: Certificate signing request (CSR) unique name initially set to "Test"
2023-07-31T12:46:27 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Config change ID 26574: item 6: Certificate signing request (CSR) Name
Test: Certificate signing request (CSR) private key PEM string added
2023-07-31T12:46:27 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Config change ID 26574: item 7: Certificate signing request (CSR) Name
Test: Certificate signing request (CSR) private key is present initially set to yes
2023-07-31T12:46:27 ex3600 mgmtd[12653]: [mgmtd.NOTICE]: AUDIT: Action ID 277605: status: completed with success
ex3600 (config) #
```

k. Ability to import X.509v3 certificates to the TOE's trust store and designate X509.v3 certificates as trust anchors / Ability to import X.509v3 certificates to the TOE's trust store:

```
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 1: System global default CA certificate 4 added
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 2: System global default CA certificate 4: CA Certifi
cate name initially set to "ICA"
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 3: The subject hash e81b420b of a default CA list cer
tificate added
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 4: The cert_id wildcard of a default CA list certific
ate with subject hash e81b420b cert_id be620044391a3551e2107ca0201b82458eebd150 added
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 5: The cert_id wildcard of a default CA list certific
ate with subject hash e81b420b cert_id be620044391a3551e2107ca0201b82458eebd150: CA subject hash ordinal symlink number initially set to 0
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 6: The cert_id wildcard of a default CA list certific
ate with subject hash e81b420b cert_id be620044391a3551e2107ca0201b82458eebd150: Default CA list cert_id initially set to "be620044391a3551e2107ca
0201b82458eebd150"
2023-08-17T10:12:05 ex3600 mgmtd[12735]: [mgmtd.NOTICE]: AUDIT: Config change ID 21519: item 7: The cert_id wildcard of a default CA list certific
ate with subject hash e81b420b cert_id be620044391a3551e2107ca0201b82458eebd150: Default CA list cert_name initially set to "ICA"
```

l. Ability to set the time which is used for timestamps:

```
2023-05-19T11:16:12 ex3600 cli[9580]: [cli.NOTICE]: AUDIT: user admin: Executing command: sh clock
2023-05-19T11:16:38 ex3600 cli[9580]: [cli.NOTICE]: AUDIT: user admin: Executing command: clock set 15:0:0
2023-05-19T11:16:38 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: requested by: user admin (System Administrator) via CLI
 (session ID 222288)
2023-05-19T11:16:38 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: descr: system clock: set time
2023-05-19T11:16:38 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: param: time of day: 15:00:00
2023-05-19T15:00:00 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: status: completed with success
2023-05-19T15:00:00 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Time change detected, clock was moved 3h 43m 21.167s forward
```

m. Ability to re-enable an Administrator account:

```
2024-05-27T10:33:42 ex3600 cli[25238]: [cli.NOTICE]: AUDIT: user admin: Executing command: aaa authentication attempts
 reset user admin2
2024-05-27T10:33:42 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Action ID 1081388: requested by: user admin (System Adm
inistrator) via CLI (session ID 23022339)
2024-05-27T10:33:42 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Action ID 1081388: descr: Unlock and reset login failur
e history of one or more users
2024-05-27T10:33:42 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Action ID 1081388: param: reset user: "admin2"
2024-05-27T10:33:42 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Action ID 1081388: status: completed with success
```

n. Ability to configure NTP:

```
2023-09-15T10:44:39 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 2465: item 1: NTP changed from disabled to enabled
2023-09-15T10:44:40 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 2466: item 1: NTP server 10.1.3.175 added
2023-09-15T10:44:40 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 2466: item 2: NTP server 10.1.3.175: initially set to enabled
2023-09-15T10:44:40 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 2466: item 3: NTP server 10.1.3.175: NTP Server keyid initially se
t to 0
2023-09-15T10:44:40 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 2466: item 4: NTP server 10.1.3.175: prefer this server initially
set to disabled
2023-09-15T10:44:40 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 2466: item 5: NTP server 10.1.3.175: NTP version initially set to
4
2023-09-15T10:44:40 ex3600 pm[7284]: [pm.NOTICE]: Launched ntpd (NTP Daemon) with pid 17814
2023-09-15T10:44:46 ex3600 pm[7284]: [pm.NOTICE]: Terminating process ntpd (NTP Daemon)
2023-09-15T10:44:46 ex3600 pm[7284]: [pm.NOTICE]: Launched ntpd (NTP Daemon) with pid 18093
2023-09-15T10:44:46 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Config change ID 2467: item 1: NTP server 10.1.3.175: NTP version changed from 4 to
 3
```

o. Ability to manage the trusted public keys database:

```
2024-06-04T10:08:32 ex3600 cli[27861]: [cli.NOTICE]: AUDIT: user admin: Executing command: ssh client user test author
ized-key sshv2 "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC3pH9GoNqZ4YiHe9YOVC+HugRJP/FYLlaO+04skcwyYdnHicxt5kirzl4DY64Sbz
Zb3nwo6BVAeOFJMKtxEx5L+dEA/pKg8LdFqIi5B1YgGS5elayBdfkJO1Vyix3uC5KI+77dIah5KgBuB6fZxIXcnGiiOvF5sSSvMpu1puIf8nS0ddW/yS0C
8ZVb7MThPODjmndBF+KyMIAmTcuMcVKuoNnbbSAjLuY7AV7iV9YVVljJycRiC0zNw3rSQd55110OOIfdhOyHCG03L2Tfd1JDStikoFOFsxkpeKKZ9KEybA
xI3Wv4F1QG0OslRgE6mjnJ6P4HX12jo0BSzsTe+GI7 root@trellixvm2"
2024-06-04T10:08:32 ex3600 mgmtd[7386]: [mgmtd.NOTICE]: Generating new hostkey of type rsa1
2024-06-04T10:08:32 ex3600 mgmtd[7386]: [mgmtd.NOTICE]: Security mode enabled: skipping hostkey of type rsa1
2024-06-04T10:08:32 ex3600 mgmtd[7386]: [mgmtd.NOTICE]: Generating new hostkey of type dsa2
2024-06-04T10:08:32 ex3600 mgmtd[7386]: [mgmtd.NOTICE]: Security mode enabled: skipping hostkey of type dsa2
2024-06-04T10:08:32 ex3600 mgmtd[7386]: [mgmtd.NOTICE]: AUDIT: Config change ID 1823: requested by: user admin (System
 Administrator) via CLI (session ID 155390), 3 item(s) changed
2024-06-04T10:08:32 ex3600 mgmtd[7386]: [mgmtd.NOTICE]: AUDIT: Config change ID 1823: item 1: SSH server record for us
er 'test' added
2024-06-04T10:08:32 ex3600 mgmtd[7386]: [mgmtd.NOTICE]: AUDIT: Config change ID 1823: item 2: SSH server record for us
er 'test': authorized key 1 added
2024-06-04T10:08:32 ex3600 mgmtd[7386]: [mgmtd.NOTICE]: AUDIT: Config change ID 1823: item 3: SSH server record for us
er 'test': authorized key 1: public key initially set to "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC3pH9GoNqZ4YiHe9YOVC+H
ugRJP/FYLlaO+04skcwyYdnHicxt5kirzl4DY64SbzZb3nwo6BVAeOFJMKtxEx5L+dEA/pKg8LdFqIi5B1YgGS5elayBdfkJO1Vyix3uC5KI+77dIah5Kg
BuB6fZxIXcnGiiOvF5sSSvMpu1puIf8nS0ddW/yS0C8ZVb7MThPODjmndBF+KyMIAmTcuMcVKuoNnbbSAjLuY7AV7iV9YVVljJycRiC0zNw3rSQd551100
OIfdhOyHCG03L2Tfd1JDStikoFOFsxkpeKKZ9KEybAxI3Wv4F1QG0OslRgE6mjnJ6P4HX12jo0BSzsTe+GI7 root@trellixvm2"
ex3600 #
```

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

a. Successful image installation:

```
2023-07-21T11:16:31 ex3600 cli[20214]: [cli.NOTICE]: AUDIT: user admin: Executing command: image install image-emps-bona-990454.img
2023-07-21T11:16:31 ex3600 mgmtd[7255]: [mgmtd.NOTICE]: AUDIT: Action ID 334012: requested by: user admin (System Administrator) via CL
I (session ID 5874836)
2023-07-21T11:16:31 ex3600 mgmtd[7255]: [mgmtd.NOTICE]: AUDIT: Action ID 334012: descr: install system software image
2023-07-21T11:16:31 ex3600 mgmtd[7255]: [mgmtd.NOTICE]: AUDIT: Action ID 334012: param: image filename: image-emps-bona-990454.img, ver
sion: emps eMPS (eMPS) 10.0.0.990454 #990454 2023-07-19 09:44:48 x86_64 build@vta922:Trellix/10.0.x-bona (eng)
2023-07-21T11:16:31 ex3600 mgmtd[7255]: [mgmtd.NOTICE]: AUDIT: Action ID 334012: param: switch next boot location after install: no
```

```
2023-07-21T11:16:31 ex3600 mgmtd[7255]: [mgmtd.NOTICE]: Installing verified image: image-emps-bona-990454.img
```

b. Image installation failure:

```
2023-06-26T10:14:40 ex3600 cli[13039]: [cli.NOTICE]: AUDIT: user admin: Executing command: image install image-emps-acumen-drop2_nosign
2023-06-26T10:14:40 ex3600 mgmtd[7357]: [mgmtd.NOTICE]: AUDIT: Action ID 55308: descr: install system software image
2023-06-26T10:14:40 ex3600 mgmtd[7357]: [mgmtd.NOTICE]: AUDIT: Action ID 55308: param: image filename: image-emps-acumen-drop2_nosign,
version: emps eMPS (eMPS) 10.0.0.988273 #988273 2023-05-22 22:45:42 x86_64 build@vta938:Trellix/10.0.x-bona (eng)
2023-06-26T10:14:40 ex3600 mgmtd[7357]: [mgmtd.NOTICE]: Installing verified image: image-emps-acumen-drop2_nosign
2023-06-26T10:14:47 ex3600 writeimage[31614]: [writeimage.ERR]: *** Could not verify image image-emps-acumen-drop2_nosign
2023-06-26T10:14:50 ex3600 mgmtd[7357]: [mgmtd.WARNING]: Exit with code 1 from writeimage.sh
2023-06-26T10:14:50 ex3600 mgmtd[7357]: [mgmtd.WARNING]: Image installation failure: *** Could not verify image image-emps-acumen-drop2
_nosign
2023-06-26T10:14:50 ex3600 mgmtd[7357]: [mgmtd.NOTICE]: Request failed: *** Could not verify image image-emps-acumen-drop2_nosign
2023-06-26T10:14:50 ex3600 mgmtd[7357]: [mgmtd.NOTICE]: AUDIT: Action ID 55308: status: completed with failure: *** Could not verify im
age image-emps-acumen-drop2_nosign
2023-06-26T10:14:51 ex3600 cli[13039]: [cli.NOTICE]: AUDIT: user admin: Executing command (image install image-emps-acumen-drop2_nosign
) failed:  % *** Could not verify image image-emps-acumen-drop2_nosign
```

V. Discontinuous changes to time - either Administrator actuated or changed via an automated process:

```
2023-05-19T11:16:12 ex3600 cli[9580]: [cli.NOTICE]: AUDIT: user admin: Executing command: sh clock
2023-05-19T11:16:38 ex3600 cli[9580]: [cli.NOTICE]: AUDIT: user admin: Executing command: clock set 15:0:0
2023-05-19T11:16:38 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: requested by: user admin (System Administrator) via CLI
 (session ID 222288)
2023-05-19T11:16:38 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: descr: system clock: set time
2023-05-19T11:16:38 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: param: time of day: 15:00:00
2023-05-19T15:00:00 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Action ID 23784: status: completed with success
2023-05-19T15:00:00 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: Time change detected, clock was moved 3h 43m 21.167s forward
```

```
2023-09-15T10:48:39 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Action ID 27561: descr: system clock: set from NTP server
2023-09-15T10:48:39 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Action ID 27561: param: NTP server: "10.1.3.175"
2023-09-15T10:48:39 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Action ID 27561: param: Authentication keyid: 0
2023-09-15T10:48:46 ex3600 mgmtd[7286]: [mgmtd.NOTICE]: AUDIT: Action ID 27561: status: completed with success
```

W. The termination of a local session by the session locking mechanism

```
2023-06-05T10:34:20 ex3600 cli[3677]: [cli.NOTICE]: AUDIT: user admin: Automatic logout due to keyboard inactivity
2023-06-05T10:34:20 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: User logout: username 'admin', full name 'System Administrator', role 'a
dmin', client 'CLI', line 'ttyl', remote hostname '(local device)', auth method 'local', auth submethod 'password', session ID 2221648
2023-06-05T10:34:20 ex3600 cli[3677]: [cli.NOTICE]: AUDIT: user admin: CLI exiting
ex3600 #
```

X. The termination of a remote session by the session locking mechanism

```
2023-05-31T07:27:45 ex3600 sshd[22737]: User admin (System Administrator) logged in via ssh2 from 10.1.3.175
2023-05-31T07:27:45 ex3600 cli[23079]: [cli.NOTICE]: user admin: CLI launched
2023-05-31T07:27:45 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: User admin (local user admin) authentication method: local (password)
2023-05-31T07:27:45 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: User login: username 'admin', full name 'System Administrator', role 'ad
min', client 'CLI', line 'pts/1', remote address '10.1.3.175', auth method 'local', auth submethod 'password', session ID 1617139
2023-05-31T07:27:45 ex3600 cli[23079]: [cli.NOTICE]: user admin: Guest-images status not available
2023-05-31T07:27:45 ex3600 cli[23079]: [cli.NOTICE]: AUDIT: user admin: Logged in with session ID 1617139
2023-05-31T07:27:45 ex3600 cli[23079]: [cli.WARNING]: user admin: Cmd reg: last word of command "_debug show detection-on-demand health
-check-duration" is of length 21, maximum ideal length is 20 (use ccf_ignore_length flag to suppress this warning if you don't want to
shorten the word)
2023-05-31T07:28:00 ex3600 su: AUDIT: (to postgres) admin on none
2023-05-31T07:28:00 ex3600 su: AUDIT: (to postgres) admin on none
2023-05-31T07:28:00 ex3600 su: AUDIT: (to postgres) admin on none
2023-05-31T07:28:45 ex3600 cli[23079]: [cli.NOTICE]: AUDIT: user admin: Automatic logout due to keyboard inactivity
2023-05-31T07:28:45 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: User logout: username 'admin', full name 'System Administrator', role 'a
dmin', client 'CLI', line 'pts/1', remote address '10.1.3.175', auth method 'local', auth submethod 'password', session ID 1617139
2023-05-31T07:28:45 ex3600 cli[23079]: [cli.NOTICE]: AUDIT: user admin: CLI exiting
```

Y. The termination of an interactive session

```
2023-06-05T10:54:21 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: User login: username 'admin', full name 'System Administrator', role 'ad
min', client 'CLI', line 'tty1', remote hostname '(local device)', auth method 'local', auth submethod 'password', session ID 2223291
2023-06-05T10:54:21 ex3600 cli[29475]: [cli.NOTICE]: AUDIT: user admin: Logged in with session ID 2223291
2023-06-05T10:54:25 ex3600 cli[29475]: [cli.NOTICE]: AUDIT: user admin: Executing command: en
2023-06-05T10:54:38 ex3600 cli[29475]: [cli.NOTICE]: AUDIT: user admin: Executing command: exit
2023-06-05T10:54:38 ex3600 mgmtd[7526]: [mgmtd.NOTICE]: AUDIT: User logout: username 'admin', full name 'System Administrator', role 'a
dmin', client 'CLI', line 'tty1', remote hostname '(local device)', auth method 'local', auth submethod 'password', session ID 2223291
2023-06-05T10:54:38 ex3600 cli[29475]: [cli.NOTICE]: AUDIT: user admin: CLI exiting
ex3600 #
```

Z. Initiation of the trusted channel

```
2023-11-09T06:16:29 ex3600 stunnel: stunnel secure channel: opened, connected to 10.1.3.175:6514 (from local interface address 10.1.3.1
73:33334)

ex3600 #
```

AA. Termination of the trusted channel

```
2023-09-14T09:56:59 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
2023-09-14T09:56:59 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
```

BB. Failure of the trusted channel functions

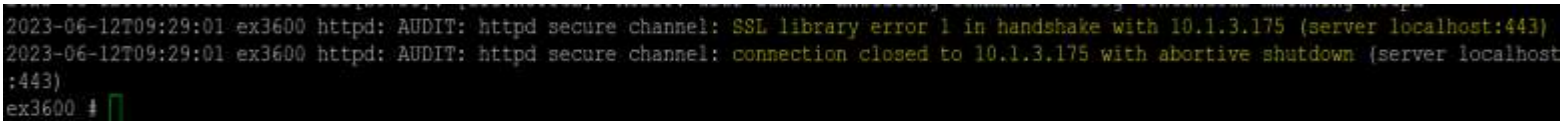
```
2023-07-25T10:27:56 ex3600 stunnel: stunnel secure channel: SSL_connect: error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number
2023-07-25T10:27:56 ex3600 stunnel: LOG3[88904484]: SSL_connect: 1408F10B: error:1408F10B:SSL routines:SSL3_GET_RECORD:wrong version number
2023-07-25T10:27:56 ex3600 stunnel: stunnel secure channel: Failed to Connect to 10.1.3.175:6514
2023-07-25T10:27:56 ex3600 stunnel: LOG3[88904485]: s_connect: connect 10.1.3.175:6514: Connection refused (111)
```

CC. Initiation of the trusted path

```
2023-09-14T09:58:34 ex3600 httpd: AUDIT: httpd secure channel: SSL connection is established with 192.168.254.169 using cipher suite ECDHE-RSA-AES
128-GCM-SHA256.
2023-09-14T09:58:34 ex3600 httpd: AUDIT: httpd secure channel: SSL connection is established with 192.168.254.169 using cipher suite ECDHE-RSA-AES
128-GCM-SHA256.
```

DD. Termination of the trusted path

EE. Failure of the trusted path functions



6 Cryptographic Protocols

Enabling CC-NDcPP compliance ensures that only certified algorithms and key sizes are available for use by the appliance.

6.1 SSH

No configuration is required other than enabling CC-NDcPP compliance. (for details see Enabling CC-NDcPP Compliance Mode of the same document)

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

6.2 TLS[10]

No configuration is required other than enabling CC-NDcPP compliance for TLS/HTTPS. (for details see Enabling CC-NDcPP Compliance Mode of the same document)

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 supports session resumption of the single HTTPS context using session tickets. The session tickets are encrypted using symmetric algorithm AES with a 128-bit key. Session tickets are structured as specified in Section 4 of RFC 5077 and encrypted using AES with a 128-bit key.

The TOE does not support certificate pinning.

The TOE will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: secp256r1, secp384r1, and secp521r1. The non-TOE server can choose to negotiate the elliptic curve from this set for any of the mutually negotiable elliptic curve ciphersuites no additional configuration is required. The TOE also supports key agreement using the server's RSA public key or DHG14 (2048 bits).

6.2.1 Reference Identifiers

The reference identifier for the syslog server is configured by the administrator using the available administrative commands in the CLI. (see section 5.3 Audit Server Configuration of the same document to see details of how to set up Audit Server)

```
Hostname (config) # Logging <reference identifier> protocol tls port
6514
```

Note: The reference identifiers must be an IPv4 address, IPv6 address, or a hostname.

When the reference identifier is a hostname, the TOE compares the hostname against all the DNS Name entries in the Subject Alternative Name extension. If the hostname does not match any of the

[10]VX series models doesn't support Web UI Feature and hence this selection-based SFR is not applicable to the VX Series Models

DNS Name entries, then the verification fails. If the certificate does not contain any DNS Name entries, the TSF will compare the hostname against the Common Name (CN). If the hostname does not match the CN, then the verification fails. For both dNSName and CN matching, the hostname must be an exact match or wildcard match. In the case of a wildcard match, the wildcard must be the left-most component, wildcard matches a single component, and there are at least two non-wildcard components.

When the reference identifier is an IP address, the TOE converts the IP address to a binary representation in network byte order. IPv4 addresses are converted directly from decimal to binary, IPv6 addresses are converted as specified in RFC 5952. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name extension. If there is not an exact binary match, then the verification fails.

The TLS channel is terminated if verification fails.

Note (from RFC 6125): IP addresses are not necessarily reliable identifiers for application services because of the existence of private internets [PRIVATE], host mobility, multiple interfaces on a given host, Network Address Translators (NATs) resulting in different addresses for a host from different locations on the network, the practice of grouping many hosts together behind a single IP address, etc.

6.3 Crypto Configuration

No configuration is required other than enabling CC-NDcPP compliance to support the values identified in the Security Target.

The following values are automatically supported when CC-NDcPP compliance is enabled and therefore do not require any action by the administrator to define or configure what is supported by the TOE.

Specifically,

- Supports the use of the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target (FCS_CKM.1).
- Supports the use of the selected key establishment schemes**.**(FCS_CKM.2).
- Supports the use of the selected modes and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption (FCS_COP.1/DataEncryption).
- Supports the use of the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services (FCS_COP.1/SigGen).
- Supports the use of the selected hash sizes for all cryptographic protocols defined in the Security Target (FCS_COP.1/Hash).
- Supports the use of the values defined in the Security Target supported by the TOE for keyed hash function, which include the key length, hash function used, block size, and output MAC length used by the HMAC function. (FCS_COP.1/KeyedHash).
- Supports the use of the RNG functionality specified in the Security Target (FCS_RBG_EXT.1).

All keys are stored plaintext and are protected from unauthorized access as the TOE stores all private keys in a secure directory that is not readily accessible to administrators.

All keys within the TSF are securely destroyed, Key is overwritten by zeros when session close or when the

compliance declassify zeroize command is issued as per mentioned in the Table 16 in ST.

7 Setting Time

This date and time are used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time can be manually updated by a Security Administrator or automatically updated using NTP synchronization. Following is the configuration needed for this.

To set the system clock, the following command is needed:

```
clock set <hh:mm:ss> [<yyyy/mm/dd>]
```

Note: The time must be specified. The date is optional; if not specified, the date will be left the same,

To set the system time zone, following command is used:

```
clock timezone <zone> [<zone word> [<zone word> [<zone word>] [<zone word>]]]
no clock timezone
```

The time zone may be specified in one of three ways:

1. A nearby city whose timezone rules to follow. The system has a large list of cities which can be displayed by the help and completion system. They are organized hierarchically because there are too many of them to display in a flat list. A given city may be required to be specified in two, three, or four words, depending on the city. The possible forms this could take include:

```
<continent> <city>
<continent> <country> <city>
<continent> <region> <country> <city>
<ocean> <island>
```

2. An offset from UTC. This will be in the form:

```
UTC-offset UTC
UTC-offset UTC-<1-12>
UTC-offset UTC+<1-14>
e.g., UTC-offset UTC-8 means the clock is 8 hours earlier than (behind) UTC.
```

3. An offset from GMT, with a counterintuitive sign. These are identical to the UTC-offset commands, except that the sign is reversed. e.g.:

```
GMT-offset GMT-8
```

means the clock is 8 hours later than (ahead of) GMT. These commands are hidden and deprecated and kept only for backward compatibility.

The default is "UTC".

To display the current system time, date and timezone. following command is required:

```
show clock
```

Note: This also shows the timezone in its internal "zoneinfo" representation, as this is the form which is accepted and displayed in the Web UI.

Set the system clock using the specified NTP server. This is a one-time operation and does not cause the

clock to be kept in sync on an ongoing basis. If authentication key is present, then request will be sent with authentication parameters (key number, keys file), by default authentication is disabled.

```
ntpdate <hostname, IPv4 or IPv6 address> [authentication key <number>]
```

Instructions to configure NTP are as follows:

To enable or disable NTP overall. The former is just a pair of aliases added to increase usability, as otherwise it may be hard for a user to figure out how to enable NTP if they are not aware of 'no' commands and only see a way to disable it.

```
ntp enable
```

```
ntp disable
```

An NTP peer may be used for synchronizing the local clock and allows the peer to potentially synchronize to the local clock. Allowable version numbers are 3 and 4. If no version number is specified when adding a peer, the default is 4.

To add or remove an NTP peer.

```
ntp peer <IPv4 or IPv6 address> [version <number>]
```

```
no ntp peer <IPv4 or IPv6 address>
```

Add or remove an NTP server. An NTP server will be used for synchronizing the local clock, without potentially influencing the server's clock. This command may be used as often as needed to install multiple NTP servers. The TOE does not place a limit on the number of NTP time sources that can be configured.
Note: Allowable version numbers are 3 and 4. If no version number is specified when adding a server, the default is 4.

```
ntp server <IPv4 or IPv6 address> [version <number>]
```

```
no ntp server <IPv4 or IPv6 address>
```

Add or remove an NTP peer. An NTP peer may be used for synchronizing the local clock and allows the peer to potentially synchronize to the local clock. This command may be used as often as needed to install multiple NTP servers. Allowable key number range is between 1 and 16. If no key is specified when adding a peer, the default is 0. Before adding the key here, it should be first configured using "`ntp authentication key`" command.

```
ntp peer <IPv4 or IPv6 address> [authentication key <number>]
```

```
no ntp peer <IPv4 or IPv6 address> authentication
```

Disable or reenable an NTP server or peer. Servers and peers start enabled; disabling is just a way of making them temporarily inactive without losing their configuration.

```
[no] ntp peer <IPv4 or IPv6 address> disable
```

```
[no] ntp server <IPv4 or IPv6 address> disable
```

Enable or disable NTP authentication overall.

```
[no] ntp authentication enable
```

Add or remove authentication keys. Key number should be configured here before using in "ntp server" command. Adding keys will overwrite the existing value present (if any). The TOE supports authentication using SHA1 as the message digest algorithm.

```
ntp authentication key <key number> hash sha1 <sha1 value>
```

```
no ntp authentication key <key number>
```

With the help of configured symmetric key and SHA1 message digest algorithm ensures the timestamp it receives from an NTP timeserver is from an authenticated source and the integrity of the time has been maintained.

Display current NTP settings.

If 'configured' is specified, the configured NTP settings will be shown. If not specified, the current runtime state of NTP is given.

```
show ntp
```

```
show ntp configured
```

Display current NTP authentication settings.

If 'configured' is specified, the configured NTP authentication settings will be shown. If not specified, the current runtime state of NTP authentication is given.

```
show ntp authentication
```

```
show ntp authentication configured
```

The NTP implementation does not accept broadcast or multicast NTP packets. No configuration is required.

8 Zeroization

Use zeroization to overwrite all passwords, keys, and non-active configuration files with zeros. There is no situation that could prevent or delay key destruction.

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
   ```

9 Self-Test

9.1 Cryptographic POST

During the cryptographic power-on self-test (POST), the appliance invokes the self-test routine provided by the cryptographic library. Appliance performs a suite of self-tests during initial start-up 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 any of the tests fail, then the appliance enters failed state and 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-NDcPP 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.
```

9.2 Software Integrity

The Software Integrity Test runs 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.

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 TOE will not start unless the tests have passed. Administrators should contact vendor support team in case of device stuck in boot loop.

10 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,

- Download the software image:

  ```
  hostname (config) # image fetch <location of image>
  ```

- View download progress:

  ```
  hostname (config) # show <location of image> image status
  ```

- Following command query the currently active version and view installation status which allows the administrator to see the installed but inactive version :

  ```
  hostname (config) # show images
  ```

- Install the downloaded software image:

  ```
  hostname (config) # image install <image-lms_7.9.0.img>
  hostname (config) # image boot next
  ```

- Save changes:

  ```
  hostname (config) # reload
  ```

- Show software version:

  ```
  hostname (config) # show version
  ```

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. The Security Administrator can query the software version running on the TOE and the most recently downloaded software version, so the TOE does support delayed activation.

Note: No functionality will cease during the update process. Device will remain fully operational until the administrator reboots the product.

11 Automatic Logout due to Inactivity[11]

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

- **For Web UI –** `webui auto-logout <minutes>`
- **For CLI –** `cli session auto-logout <minutes>`

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

[11] VX series appliances don't support WEB UI feature

12 Login Banners

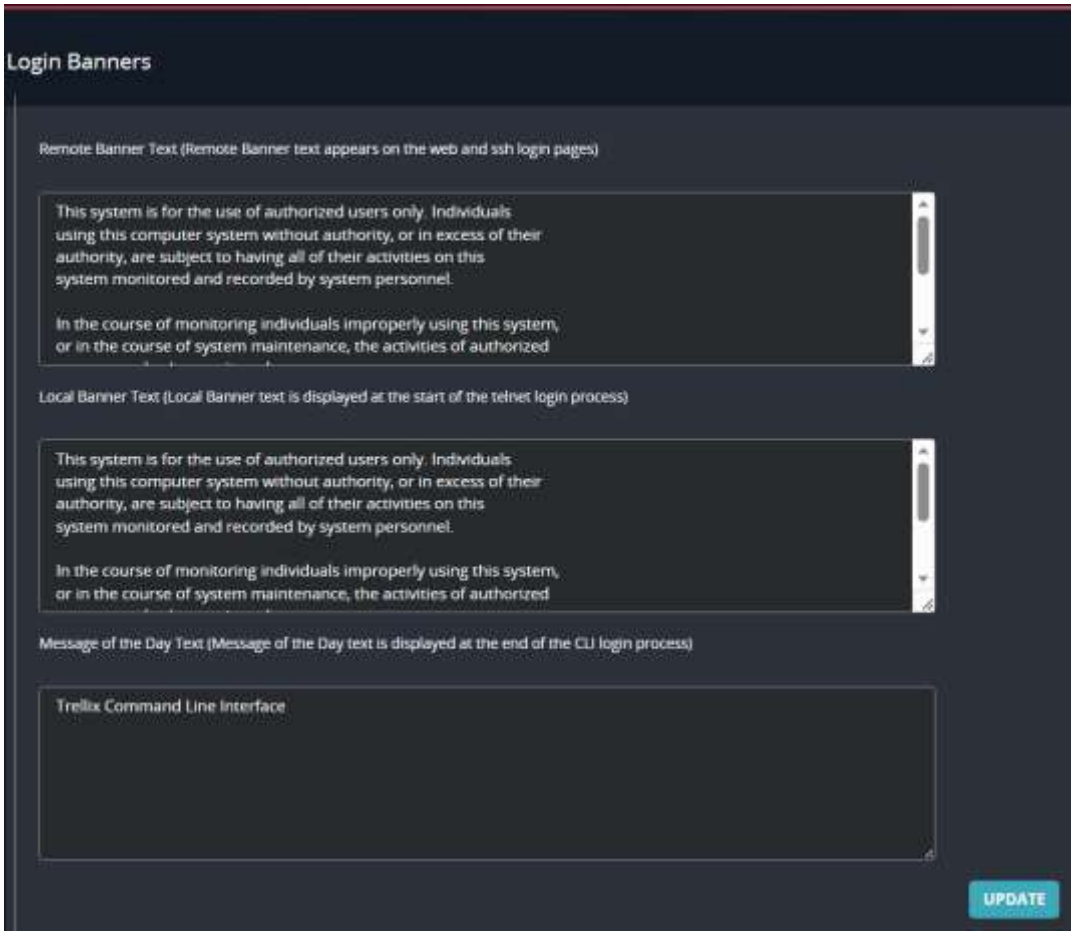
You can customize or remove the messages that appear when users log in to the TOE. You can configure three messages:

- **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.

Note: Display of the Login banner is the only service that is available prior to identification and authentication. No configuration is required to ensure that access to services is limited prior to login.

12.1 Customizing Login Banners and Messages Using the Web UI[12]

Use the **Login Banner** page to configure the messages users see when they log in to the NX Series appliance.



12.2 Customizing Login Banners and Messages Using the CLI

[12] VX series appliances don't support WEB UI feature

To configure the messages which users see when they log in to the appliance:

- To change the local login message only, use the following command:
  ```
  hostname (config) # banner login-local "<text>"
  ```
- To change the remote login message only, use the following command:
  ```
  hostname (config) # banner login-remote "<text>"
  ```
- To change the message of the day, use the following command:
  ```
  hostname (config) # banner motd "<text>"
  ```
- To clear the local login message, the remote login message, or both:
  ```
  hostname (config) # banner login "<text>"
  hostname (config) # banner login-local "<text>"
  hostname (config) # banner login-remote "<text>"
  ```
- To clear the message of the day:
  ```
  hostname (config) # banner motd "<text>"
  ```
- To restore the default messages:
  ```
  hostname (config) # no banner login
  hostname (config) # no banner motd
  ```
- Save changes.
  ```
  hostname (config) # write memory
  ```

---End of Document---