Extreme™
Customer-Driven Networking

CONFIGURATION GUIDE

Network OS Common Criteria

Supporting Network OS v7.3.0aa

9035610
December 2018

Contents

Preface **5**

- Document conventions 5
  - Notes, cautions, and warnings 5
  - Text formatting conventions 5
  - Command syntax conventions 6
- Extreme resources 6
- Document feedback 6
- Contacting Extreme TechnicalSupport 7
- Supported hardware and software 8

Common Criteria Certification **9**

- Common Criteria overview 9
- Establishing a serial connection 10
- Setting the Management IP address of the Device 11
- Device Access 11
- Common Criteria preparationoverview 12
  - Configuring Common Criteria mode 13
- Downloading firmware from Extreme's website 17
  - Firmware update 17
- Password Requirements 19
- Setting System Date and Time 19
- REST API usage 20
- TLS server certificateauthentication 20
  - TLS cipher suites for client and server applications 20
  - Verify the revocation status of certificate using OCSP 21
- NETCONF logging support 21
- REST logging support 21
  - Configuring SSH session rekey interval by volume and time 23
- Audit Logs 24
  - SYSLOG server configuration 24

Appendix A: Audit Log Entries **25**

Preface

- Document conventions
- Extreme resources
- Document feedback
- Contacting Extreme Technical Support
- Supported hardware and software

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Extreme technical documentation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.
`Courier font`	Identifies CLI output.
	Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Extreme resources

Visit the Extreme website to locate related documentation for your product and additional Extreme resources.

White papers, data sheets, and the most recent versions of Extreme software and hardware manuals are available at www.extremenetworks.com. Product documentation for all supported releases is available to registered users at www.extremenetworks.com/support/documentation.

Document feedback

Quality is our first concern at Extreme, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you.

You can provide feedback in two ways:

- Use our short online feedback form at http://www.extremenetworks.com/documentation-feedback-pdf/
- Email us at internalinfodev@extremenetworks.com

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Contacting Extreme Technical Support

As an Extreme customer, you can contact Extreme Technical Support using one of the following methods: 24x7 online or by telephone. OEM customers should contact their OEM/solution provider.

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for immediate support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact.
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge - Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub - A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal - Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve theproblem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Supported hardware and software

In those instance in which procedures or parts of procedures documented here apply to some devices but not to others, this guide identifies exactly which devices are supported and which are not.

Although many different software and hardware configurations are tested and supported by Extreme Networks, Inc. for Network OS, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of Network OS:

- ExtremeSwitching VDX 6740-48
- ExtremeSwitching VDX 6740T
  - ExtremeSwitching VDX6740T-64
  - ExtremeSwitching VDX 6740T-1G
- ExtremeSwitching VDX 6940-144S
- ExtremeSwitching VDX 6940-36Q
- ExtremeSwitching VDX 8770
  - ExtremeSwitching VDX8770-4
  - ExtremeSwitching VDX8770-8

To obtain information about a Network OS version other than this release, refer to the documentation specific to that version.

Common Criteria Certification

- Common Criteria overview
- Establishing a serial connection
- Setting the Management IP address of the Device
- Device Access
- Common Criteria preparationoverview
- Downloading firmware from Extreme's website
- Password Requirements
- Setting System Date and Time
- REST API usage
- TLS server certificateauthentication
- NETCONF logging support
- REST logging support
- Audit Logs

Common Criteria overview

This section contains steps for configuring the Extreme Networks OS switch for Common Criteria (CC) standards with Network OS version 7.3.0aa collaborative Protection Profile for Network Devices (cNDPP) version 2.0.

Common Criteria certification for a device enforces a set of security standards and feature limitations on a device to be compliant with the Common Criteria standards, similar to placing the device in FIPS mode. To better understand the Common Criteria certification and the associated security functions that have been subject to certification, refer to the document *Extreme Switches NOS 7.3.0aa (cNDPP) Security Target*.

The Network OS device management functions are isolated through authentication. Once administrators log in with specific credentials, their access is limited to commands for which they have privileges and role-based permissions. Additionally, network management communication paths are protected against modification and disclosure using SSHv2. The audit channel to an external Syslog server is protected using TLS encapsulation.

FIPS 140-2 Security Level 1 specifies the security requirements that are satisfied by a cryptographic module utilized within a security system protecting sensitive information of the system.

Extreme Network OS switches running Network OS 7.3.0aa are designed to support FIPS-compliance mode. All cryptographic algorithms required and used in CC are certified by the Cryptographic Algorithm Validation System (CAVS). The RNG component does not require configuration and follows the specified requirements as above.

Establishing a serial connection

Perform all configuration tasks in this guide using a serial connection from a workstation or terminal. The serial port can be used to connect to a workstation to configure the IP address for the device before connecting it to a fabric or IP network.

Complete the following steps to create a serial connection to the device.

1. Connect the serial cable to the serial port on the device and to an RS-232 serial port on the workstation or terminal device.
If the serial port on the workstation or terminal device is RJ-45 instead of RS-232, remove the adapter on the end of the serial cable and insert the exposed RJ-45 connector into the RJ-45 serial port on the workstation.

2. Open a terminal emulator application (such as HyperTerminal on a PC, or TERM, TIP, or Kermit in a UNIX environment), and configure the application as follows:

- In a Windows environment, enter the following values: 9600 bits per second, 8 databits, no parity, 1 stop bit, and no flow control.

NOTE

Flow control is not supported on the serial consoles when attached to remote terminal servers and must be disabled on the customer-side remote terminal server and the host-side clients.

- In a UNIX environment using TIP, enter the following string at the prompt:

```
# tip /dev/ttyb -9600
```

If ttyb is already in use, use ttya instead.

The serial port is located on the port side of the chassis. The Extreme VDX 6740, VDX 8770, VDX 6940-36Q, and VDX 6940-144 uses an RJ-45 connector for the serial port.

The Extreme VDX 6740T, 6740-T-1G uses a mini-USB connector for the serial port. An RJ-45 to DB9 adapter is also provided with each model. The cable supplied is a rollover cable.

CAUTION

To protect the serial port from damage, keep the cover on the port when not in use.

Refer to the product Technical Specifications for a listing of serial cable pinouts.

Serial port specifications (pinout mini-USB)

Pin	Signal	Description
1	+5V	Not used
2	UART0_TX	Debug port
3	UART0_RX	Console port
4	IN	Not used
5	GND	Ground

Serial port specifications (pinout RJ-45)

Pin	Signal	Description
1	Not supported	N/A
2	Not supported	N/A
3	UART1_RXD	Receive data
4	GND	Logic ground
5	GND	Logic ground
6	UART1_TXD	Transmit data
7	Not supported	N/A
8	Not supported	N/A

Serial port specifications (protocol)

Parameter	Value
Baud	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

Setting the Management IP address of the Device

Once the device is accessible through a serial interface, the IP address of its management interface can then be configured so that various network functions can be performed. This configuration can be done through the following steps:

```
device # configure
Entering configuration mode terminal

sw0(config)# interface Management 1/0
sw0(config-Management-1/0)# ip address [10.24.12.139/22 || dhcp]
```

where a static IP address can be provided or the ‘dhcp’ keyword used to use the IP address provided by a DHCP server.

The IP address of the interface can be removed by using the ‘no’ form of the ‘ip address’ command.

Device Access

A VDX device can be accessed or managed using various options. These include console access (over serial interface), SSH, REST requests as well as NETCONF requests. The serial connection is described above in Establishing a serial connection.

To access the device using SSH from a remote client:

```
remote-device-prompt# ssh <IP-address-of-VDX-device>
```

The appropriate user credentials must be provided to gain access to the device. The connection can be terminated by giving the ‘exit’ command from the shell.

To send and receive NETCONF request to the device, the device is accessed over an SSH connection and specifying the NETCONF port as in the example below:

```
remote-device-prompt# ssh admin@10.24.12.151 -p 830 -s netconf
```

The session is closed by sending <close-session> RPC or by terminating the corresponding ssh connection.

Once the HTTPS server is configured, an HTTPS request can then be sent to the server along with the appropriate user credentials. If the credentials are valid, the HTTPs server will provide a reply over the secure channel.

By default, administrator access to the device is unaffected by the maximum login failure limit. However, if the password attributes are modified to enable administrator lockout and the administrator provides the incorrect credentials after the specified number of retries, the administrator will only be able to log in over the network after the lockout duration has elapsed.
To enable administrator lockout:

```
device# configure terminal
device(config)# password-attributes admin-lockout
device(config)# password-attributes max-retry 4
device(config)# password-attributes max-lockout-duration <0-99999> (in minutes)
```

Note that administrator logins over the serial port/console is never locked out. The admininstrator can login over the network again if the admin-lockout password attribute is disabled.

To allow the administrator to login over the network and disable administrator lockout:

```
device# configure terminal
device(config)# no password-attributes admin-lockout
```

Common Criteria preparation overview

The steps to configure the TOE to support Common Criteria requirements can only be performed by a user with administrative privileges. The following steps summarize the Common Criteria configuration process:

1. Enable the KATs and the conditional tests (including pairwise consistency tests).
2. Zeroize and reboot the switch into the FIPS-compliant state.
3. Enable strict password checking.
4. Configure CC-compliant ciphers for SSH.
5. Configure timeouts for SSH client connections to the SSH server in the device.
6. Configure other required SSH configurations, such as the maximum time that an SSH client can stay idle, maximum login attempts, and maximum login timeout.
7. Restart the SSH server to apply the configuration.
8. Configure IP ACLs to block HTTP and Telnet ports.
9. Remove configurations of unsupported features TACACS+,RADIUS and LDAP.
10. For authentication by a Microsoft Active Directory server, import the LDAP CA certificate for LDAP authentication.
11. To support TLS for Syslog, import the CA certificate of the Syslog server.
12. To support SSH public-key authentication, import the public key.
13. Disable the Telnet server.

Configuring Common Criteria mode

To configure the Extreme Network OS switch for CC compliance mode, execute the following steps.

> **NOTE**
>
> Configuring an Extreme Network OS switch for CC compliance mode using NETCONF operations is not supported. NETCONF interface must be blocked before configuring the CC compliance mode.

1. Log in to the switch as admin.
2. Enter the **unhide fips** command. Contact Extreme GTAC for the password.

   ```
   device# unhide fips
   ```

   You will have access to all FIPS commands, such as the **fips zeroize** command.
3. Enter the **fips selftests** command to move the crypto module to FIPS mode.

   > **NOTE**
   >
   > This command cannot be undone.

   ```
   device#fips selftests
   ```

4. Enter the **fips zeroize** command to zeroize all the existing security configurations and parameters.The operation to clear out all keys are performed immediately.

   > **NOTE**
   >
   > This command prompts the user for permission to continue. It copies the default configuration to the startup configuration and reloads the device.

   ```
   device# fips zeroize
   This operation erases all passwords, shared secrets,
   private keys, and entire Dcmd configuration etc. on the switch.
   ```

5. Configure the system for crypto compliance.

   a) Enter global configuration mode.

   ```
   device# configure terminal
   ```

   b) Enable strict password checking by issuing the following commands.

   ```
   device(config)# password-attributes min-length 8

   device(config)# password-attributes max-retry 4
   device(config)# password-attributes max-lockout-duration 5000
   device(config)# password-attributes character-restriction upper 1
   device(config)# password-attributes character-restriction lower 2
   device(config)# password-attributes character-restriction numeric 1
   device(config)# password-attributes character-restriction special-char1
   ```

   By default, the administrator is not locked out of the device even after ‘`max-retry`’ failures. To lock the administrator out, execute this command:

   ```
   device(config)# password-attributes admin-lockout
   ```

   When the administrator is locked-out, the device will only allow access for the administrator after the value set for ‘`max-lockout-duration`’.

   The command above requires the user to provide a strong password.

   c) Enter the **ssh server key-exchange** command to configure the SSH Server key-exchange protocol.

   ```
   device(config)# rbridge-id 1
   device(config-rbridge-id-1)# ssh server key-exchange diffie-hellman-group14-sha1
   ```

d) Enter the following commands to remove the SSH DSA host key and ECDSA host key.

```
device(config-rbridge-id-1)#  ssh server key dsa
device(config-rbridge-id-1)#  ssh server key ecdsa 256
device(config-rbridge-id-1)#  no ssh server key ecdsa 256
```

e) Enter the **ssh server cipher** command to configure the SSH server cipher.

```
device(config-rbridge-id-1)# ssh server cipher aes128-ctr,aes256-ctr,aes128-cbc,aes256-cbc
```

f) Enter the **ssh server max-idle-timeout** command to set the timeout value for SSH connections to the server.

```
device(config-rbridge-id-1)# ssh server max-idle-timeout 20

Note:
The SSH session Idle timeout will work only if it is less than the rekey timeout because the
rekeying messages disrupt the idle state

From user experience point of view at times user may not see the idle timeout disconnecting the
SSH session even when it is less than rekey timeout but closer to the Rekey timeout, because the
session may not have actually idled for the configured period of time and gets disrupted by the
rekeying.

For e.g if Idle timeout is configured as 890 seconds and rekey timeout is configured as 900
seconds leaving a gap of 10secs b/w them, when user starts the session and takes more than 10
seconds to login, the idling starts after authentication, but the rekey timer has ticked off
immediately after the key exchange. Hence user will see a rekeying the first time when he
immediately idles after authentication.

Similarly if user sends data after 100 seconds of idling(immediately after rekey) and session
starts idling at 105th second, the time left for next rekeying is 900-105 =795. Hence a rekeying
occurs before idle timeout and user will see the next idle timeout disconnecting the session at
795 + 890 = 1685 secs.

In general the idle-timeout should be less than the rekey timeout for it to work, and for better
user experience it should not be close to the rekey timeout (will leave a gap of 5 seconds
atleast)

We could default to no rekeying by providing “no ssh server rekey-interval”which sets default 0
and prevents rekeying, and thus have idle timeout give the right user experience.

In case we want the timeout to give the right user experience with rekey timer ON
Then user could use the below command to specify inactivity timeout

Device(config)line vty exec-timeout 100
```

g) Enter the **ssh server max-auth-tries** command to set the number of login attempts.

```
device(config-rbridge-id-1)# ssh server max-auth-tries 2
```

h) Enter the **ssh server max-login-timeout** command to set the login timeout. Set the value to an appropriate timeout period in the administrator’s environment.

```
device(config-rbridge-id-1)# ssh server max-login-timeout 30
```

i) If the device is in FIPS-mode, any changes to ssh-server will require a restart as the SSH server cannot be restarted by itself. Otherwise, enter the **ssh server shutdown** and **no ssh server shutdown** commands to restart the SSH server.

```
device(config-rbridge-id-1)# ssh server use-vrf mgmt-vrf shutdown
device(config-rbridge-id-1)# ssh server use-vrf default-vrf shutdown
device(config-rbridge-id-1)# no ssh server use-vrf mgmt-vrf shutdown
device(config-rbridge-id-1)# no ssh server use-vrf default-vrf shutdown
```

j) Enter the CA Certificate import command and enter http server shutdown and no http server shutdown commands to restart the HTTP server to enable HTTPS.

```
device(config-rbridge-id-1)# crypto key label mykey1 rsa modulus 2048

device(config-rbridge-id-1)# crypto ca trustpoint trust1

device(config-ca-t1)#keypair mykey1
device(config-ca-t1)# exit

device#crypto ca authenticate trust1 cert-type https protocol SCP host 10.24.15.200 directory /root/
 jdoe/certs file ca.cert.pem user root password pass

device#crypto ca enroll trust1 cert-type https protocol SCP country US state CA locality San Jose
 organization Engg orgunit Engg common jdoe directory /root/jdoe/certs host 10.24.15.200 user root
 password pass

device#crypto ca import trust1 certificate cert-type https protocol SCP directory /root/jdoe/certs
 file jdoe.pem host 10.24.15.200 user root password  pass
 device(config-rbridge-id-1)# http server use-vrf mgmt-vrf shutdown
 device(config-rbridge-id-1)# http server use-vrf default-vrf shutdown
 device(config-rbridge-id-1)# no http server use-vrf mgmt-vrf shutdown
 device(config-rbridge-id-1)# no http server use-vrf default-vrf shutdown
```

6. Use IP ACLs to block Telnet, HTTP, and Extreme internal ports 7110, 7710, 8008, 9110, and 9710 for IPv4 and IPv6. If SSH access is required, enter **seq permit** commands to allow access on port 22. If remote access is required, such as through SCP or LDAP, enter **seq permit** commands to allow UDP and TCP traffic on ports 1024 through 65535. Configure IP ACLs using the **ip access-list** command and use the **ip access-group** command to apply the rules to the management interface.

```
device(config)# ip access-list extended ccextACL
device(config-ip-ext)# seq 1 deny tcp any any eq 23
device(config-ip-ext)#seq 2 deny tcp any any eq 80
device(config-ip-ext)#seq 5 deny tcp any any eq 7110
device(config-ip-ext)#seq 6 deny tcp any any eq 7710
device(config-ip-ext)#seq 7 deny tcp any any eq 8008
device(config-ip-ext)#seq 8 deny tcp any any eq 9110
device(config-ip-ext)#seq 9 deny tcp any any eq 9710
device(config-ip-ext)#seq 11 permit tcp any any range 1024 65535
device(config-ip-ext)#seq 12 permit udp any any range 1024 65535
device(config-ip-ext)#seq 13 permit tcp any any eq 22
device(config-ip-ext)#seq 14 permit tcp any any eq 830
device(config-ip-ext)#exit
device(config)# interface management 1/0
device(config-Management-1/0)# ip access-group ccextACL in

device(config)# ipv6 access-list extended ccextACL6
device(config-ip-ext)# seq 1 deny tcp any any eq 23
device(config-ip-ext)#seq 2 deny tcp any any eq 80
device(config-ip-ext)#seq 5 deny tcp any any eq 7110
device(config-ip-ext)#seq 6 deny tcp any any eq 7710
device(config-ip-ext)#seq 7 deny tcp any any eq 8008
device(config-ip-ext)#seq 8 deny tcp any any eq 9110
device(config-ip-ext)#seq 9 deny tcp any any eq 9710
device(config-ip-ext)#seq 11 permit tcp any any range 1024 65535
device(config-ip-ext)#seq 12 permit udp any any range 1024 65535
device(config-ip-ext)#seq 13 permit tcp any any eq 22
device(config-ip-ext)#seq 14 permit tcp any any eq 830
device(config-ip-ext)#exit
device(config)# interface management 1/0
device(config-Management-1/0)# ipv6 access-group ccextACL6 in
```

NOTE

Do not use FTP mode for the following operations: copying startup or running configuration, copy support, and firmware download.

7. Enter the **no tacacs-server** command to remove any TACACS+ server configuration.

```
device(config)# no tacacs-server <host>
```

8. Enter the **no radius-server** command to remove any RADIUS serverconfiguration.

```
device(config)# no radius-server <host>
```

9. To enable secure logging using the syslog server, complete the following steps.

   a) Enter the **crypto import syslogca** command in privileged EXEC mode to import the syslog CA certificate.

   ```
   device# crypto import syslogca rbridge-id 1 protocol SCP host 10.2.2.101 directory /home/certs/
   file chainCA02.cert.pem user admin password <password>
   ```

   The CA certificate imported must be generated using RSA-2048 with SHA-256.

   b) Enter the **logging syslog-server** *ip-address* command in global configuration mode to configure the syslog server.

   ```
   device(config)# logging syslog-server 10.20.238.120 secure port 1999
   ```

   The device will enforce certificate validation during import. Details of the enforcement are provided in the section "TLS server certificate authentication" later in this document.

10. To use SSH public-key authentication, enter the **certutil import sshkey directory** *pubkey-directory* **file** *filename* **protocol SCP host** *remote-ip* **user** *user-account password password* command to import the public key.

```
device# certutil import sshkey user admin host 10.70.4.106 directory /users/home40/bmeenaks/.ssh
file id_rsa.pub login fvt
Password: ***********
 2012/11/14-10:28:58, [SEC-3050], 75,, INFO, VDX, Event: sshutil, Status: success, Info: Imported
SSH public key from 10.70.4.106 for user 'admin'.
```

To support passwordless SSH authentication, externally generated key pairs using RSA-2048.

11. Enter the **telnet server shutdown** command in global configuration mode to disable the Telnet server.

```
device(config-rbridge-id-1)# telnet server shutdown
```

12. An optional step is to configure banner messages. The banner messages are used to provide information to the user when the TOE is accessed. There are three commands that can be used to setup banner messages. These are:

- banner incoming – sets the incoming banner message. The message is seen on the console when a user accesses the device
- banner motd – sets the message of the day banner. The message is displayed when the device receives a login request. Also used to display a message for other users of the switch.
- banner login – sets the switch banner and the message is displayed after the user is authenticated.

Banner length is from 1 – 2048 characters. Characters can be issued as a single line of text, or in multiline mode by pressing esc m.

Each of these commands can be invoked from the CLI in configure mode as

```
device # banner incoming <message>
device # no banner incoming
device # banner motd <message>
device # no banner motd
device # banner login <message>
device # no banner login
```

13. Enter the **copy running-config startup-config** command to save all settings to the startup configuration file.

```
device# copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue? [Y/N]: Y
```

Downloading firmware from Extreme's website

Perform the following tasks to download the firmware.

1. Extreme uploads the signed firmware as a tar file with its associated MD5 on secure location.

   NOTE

   File location and version details are provided to the customer.

Download and verify with downloaded image with md5sum, or other md5 checksum utility.

Firmware update

Firmware packages are signed using the 2048-bit RSA key with SHA-256 during firmware build and verified during firmware installation as specified in the following steps. Note that the TOE only supports firmware updates that completely replace the existing firmware (i.e., all packages).

1. The digital signatures of various packages are downloaded first and used for package validation.
2. As part of firmware download, each package is validated by verifying the signature. This process is done by the TOE without administrator intervention. There is no visible way to see that these files are being validated. If a file cannot be verified, the installation fails with

   ```
    "error (62)" type show firmwaredownloadstatus to see the status messages. I.E: "[2]: Wed Sep
   26 18:06:37 2018 Slot SW/0: Firmware install ends. Failed to validate firmware signature.(62)"
   The firmware will recover automatically to the version that was installed prior to attempting
   to upgrade. This is recorded in show firmwaredownloadstatus as follows.   "[5]: Wed Sep 26
   18:06:48 2018 Slot SW/0: Firmware download failed but it has recovered successfully."
   ```

3. Installation begins after the packages are validated.
4. By default, **firmware download** downloads the firmware to the system, reboots the system, and commits the firmware automatically.. When the firmware is installed and the device is rebooted, the administrator must wait until the device reports that commands can be accepted through the CLI. Also, device functions will be affected until the device reports that the firmware upgrade has been successfully completed.

Firmware download

Syntax

firmware download { default-config | ftp | scp | sftp | usb | interactive } [manual] [coldboot] host { hostname | host_ip_address } user username password password directory directory [file file_name] [vcs-mode vcsmode] [vcs-id vcsID] [rbridge-id rbridge-id]]

Command Default   By default, firmware download downloads the firmware to the system, reboots the system, and commits the firmware automatically.

Parameters

default-config

Sets the configuration back to default except for the following parameters:
Management IP and gateway, VCS ID, and RBridge ID. These three parameters are retained except when the options to change their values are specified.

ftp | scp | sftp | usb

Valid protocols are
ftp (File Transfer Protocol) or scp (Secure Copy), sftp (SSH File Transfer Protocol), usb (universal serial bus). The values are not case-sensitive.

interactive

Runs firmware download in interactive mode. You are prompted for input.

manual

Updates a single management module in a chassis with two management modules. You must log in to the management module through its dedicated management IP address. This parameter is ignored when issued on a Top-of-Rack (ToR) switch or in a chassis with only one management module.

coldboot

Downloads the firmware to the system and reboots both the active and standby MMs. / partitions. This results in a full reboot of the unit.

host

	Specifies the host by DNS name or IP address.
Hostname	Specifies an IPv4 DNS host name.
host_ip_address	Specifies the host IP address. IPv4 and IPv6 addresses are supported.
Directory	directory

NOTE

If the installation fails, an error with details is displayed and the download procedure is terminated and recovered to version installed prior to attempting to upgrade.

The public key file on the switch contains only one public key. It is only able to validate firmware signed using one corresponding private key. If the private key changes in future releases, you must change the public key on the switch by using the **firmware download** command. When a new firmware is downloaded, the firmware download always replaces the public key file on the switch with what is in the new firmware. This allows you to have planned firmware key changes.

You can download the signed firmware with its associated MD5 from www.extremenetworks.com.

Firmware Version Installed

The installed firmware version can be displayed from the CLI by

```
device# show version

Network Operating System Software
Network Operating System Version: 7.3.0d
Copyright (c) 1995-2018 Extreme Networks
Firmware name:      7.3.0d
Build Time:         14:39:28 Sep 20, 2018
Install Time:       15:35:06 Sep 20, 2018
Kernel:             2.6.34.6

BootProm:           1.0.1
Control Processor: e500mc with 8192 MB of memory

Slot    Name    Primary/Secondary Versions                         Status
---------------------------------------------------------------------------
SW/0    NOS     7.3.0d                                              STANDBY
                7.3.0d
SW/1    NOS     7.3.0d                                              ACTIVE*
                7.3.0d
```

To display the crypto library information,

```
device# unhide fips

device# show fips
```

Password Requirements

Minimum password attributes are required to satisfy the Approved mode. These attributes include the minimum length, character sets, the number of retries when logging in and how long an account can be locked out when the maximum number of login failures is observed.

These minimum password length is eight (8) characters and the password should have at least one(1) upper-case character, two(2) lower-case characters, one(1) numeric character and one(1) special character from the set of all printable, non-alphanumeric punctuation characters except the colon (:) are allowed.

The steps to configure the password requirements are listed in Configuring Common Criteria mode.

Setting System Date and Time

To manually set the system date and time, the following command can be used from the CLI:

```
device# clock set CCYY-MM-DDTHH:MM:SS [ rbridge-id { rbridge-id | all } ]
```

where

CCYY-MM-DDTHH:MM:SS

Specifies the local clock date and time in year, month, day, hours, minutes, and seconds. Valid date and time settings range from January 1, 1970 to January 19, 2038.

rbridge-id

Specifies an RBridge or all RBridges.

rbridge-id

Specifies an RBridge ID.

all

Specifies all RBridges.

REST API usage

REST is an administrative interface available for remotely managing NOS.

REST web service leverages HTTP by default but this is changed to use HTTPS when in approved mode, and uses its standard methods to perform the operations on the device. A web server embedded in the VDX switches is used to serve the REST API to the clients.

In order to enable the HTTPS server, the configuration is described in Configuring Common Criteria mode.

Once the HTTPS server is configured, an HTTPS request can then be sent to the server along with the appropriate user credentials. If the credentials are valid, the HTTPs server will provide a reply over the secure channel.

TLS server certificate authentication

TLS server certificate validation occurs during the TLS handshake according to the following rules:

- Certificate validation and the certificate path validation support a minimum path length of three certificates.
- The certificate path must terminate with a trusted CA certificate.
- The certificate path should be validated by verifying the presence of the `basicConstraints` extension and that the CA flag is set to TRUE for all CA certificates.
- The revocation status of the certificate should be validated.
- For Syslog, the device currently requires that an IP address must be used for Common Name (CN) and Subject Alternative Name (SAN).
- The `extendedKeyUsage` field should be validated according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification should have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the `extendedKeyUsage` field.
  - Server certificates presented for TLS should 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 should 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 should have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the `extendedKeyUsage` field.
- A certificate should only be treated as a CA certificate if the `basicConstraints` extension is present and the CA flag is set to TRUE.

Users will be notified using Raslog/Auditlog with the reason for the TLS server certificate validation failure during TLS handshake, if applicable.

TLS cipher suites for client and server applications

The TLS cipher suites used by the client and server applications by the TOE are preset and cannot be changed through CLI commands. These cipher suites are as follows:

TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
***TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*.**

Verify the revocation status of certificate using OCSP

The switch will always perform OCSP revocation-check on the certificate when the `authorityInfoAccess` extension is present and indicates that the `accessMethod` to use is OCSP(1.3.6.1.5.5.7.48.1) specifying the `accessLocation` which is the URI of the OCSP responder.

Only when the revocation status is *'good'* that the certificate will be accepted.

When the switch cannot establish a connection to the determine the validity of a certificate, then it will not accept the certificate.

NETCONF logging support

When the NETCONF RPC request/responses are issued by the user, then all request/responses (including payload) are logged. These includes all the RPC requests received and responses generated. This log is accessible as part of the **supportsave** command.

```
device# copy support scp host <remote-host-ip-address> directory <dir> user <usr> rbridge-id <1>
use-vrf <vrf-name>
```

The following is a sample of a NETCONF log:

```
27-Jan-2017::22:54:46.617 **> sess:18 read:
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:netconf:base:1.0</capability>
  </capabilities>
</hello>

]]>]]>
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <get-config>
    <source>
      <running/>
    </source>
    <filter type="subtree">
      <snmp-server xmlns="urn:extremenetworks.com:mgmt:extreme-snmp"/>
    </filter>
  </get-config>
</rpc>

27-Jan-2017::23:00:32.687 **< sess:18 write:
<rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <snmp-server xmlns="urn:extremenetworks.com:mgmt:extreme-snmp">
      <agtconfig>
        <sys-descr>Extreme BR-SLX9540 Router</sys-descr>
      </agtconfig>
      <enable>
        <trap>
          <trap-flag/>
        </trap>
      </enable>
    </snmp-server>
  </data>
</rpc-reply>
```

REST logging support

When the REST queries are issued, the query is logged. This contains the information about the timestamp, URI, payload, METHOD, http version, the Host IP, user and the Http status code of the result for the corresponding query. The log is available as part of the **supportsave** command.

```
device# copy support scp host <remote-host-ip-address> directory <dir> user <usr> rbridge-id <1>
use-vrf <vrf-name>
```

All the positive and negative test cases are logged. However, if any crashes occur when the query is issued, it is not logged.

The log entries follow this format:

<Timestamp> <username> <Httpversion> <Method> <URI> <Payload> <Http-response-status>

The following is a sample of a REST log:

```
Fri Sep 29 11:43:22 2017 : 10.70.6.202  admin    HTTP/1.1 GET  /rest/config/running/router/mpls/policy
404 Not Found
Fri Sep 29 11:46:01 2017 : 10.70.6.202  admin    HTTP/1.1 Uknown  /rest/config/running/router/mpls/policy
405 Method Not Allowed
Fri Sep 29 11:46:08 2017 : 10.70.6.202  admin    HTTP/1.1 Uknown  /rest/config/running/router/mpls/policy
405 Method Not Allowed
Fri Sep 29 11:46:18 2017 : 10.70.6.202  admin    HTTP/1.1 PUT  /rest/config/running/router/mpls/policy
200 OK
Fri Sep 29 18:22:02 2017 : 10.70.6.202  admin    HTTP/1.1 GET  /rest/config/running    200 OK
Fri Sep 29 18:22:14 2017 : 10.70.6.202  admin    HTTP/1.1 GET  /rest/config/running1    404 Not Found
Fri Sep 29 18:22:29 2017 : 10.70.6.202  admin    HTTP/1.1 Uknown  /rest/config/running    405 Method Not
Allowed
Fri Sep 29 18:26:17 2017 : 10.70.6.202  admin    HTTP/1.1 POST  /rest/config/running/router <mpls/>    200 OK
Fri Sep 29 18:26:56 2017 : 10.70.6.202  admin    HTTP/1.1 GET  /rest/config/running    200 OK
Fri Sep 29 18:29:06 2017 : 10.70.6.202  admin    HTTP/1.1 POST /rest/config/running/router/mpls <mpls/>
400 Bad Request
Fri Sep 29 18:35:18 2017 : 10.70.6.202  admin    HTTP/1.1 POST  /rest/config/running/router/mpls/policy
<policy><retry-time>21</retry-time></policy>   400 Bad Request
Fri Sep 29 18:35:33 2017 : 10.70.6.202  admin    HTTP/1.1 PATCH  /rest/config/running/router/mpls/policy
<policy><retry-time>21</retry-time></policy>   200 OK
Fri Sep 29 18:36:44 2017 : 10.70.6.202  admin    HTTP/1.1 PATCH  /rest/config/running/router/mpls/policy1
<policy><retry-time>21</retry-time></policy>   400 Bad Request
Fri Sep 29 18:37:58 2017 : 10.70.6.202  admin    HTTP/1.1 PUT /rest/config/running/router/mpls/policy/cspf-
interface-constraint    406 Not Acceptable
Fri Sep 29 18:39:00 2017 : 10.70.6.202  admin    HTTP/1.1 PUT /rest/config/running/router/mpls/policy/cspf-
interface-constraint <cspf-interface-constraint>true</cspf-interface-constraint>   200 OK
Fri Sep 29 18:40:01 2017 : 10.70.6.202  admin    HTTP/1.1 DELETE  /rest/config/running/router/mpls/policy
200 OK
Fri Sep 29 18:40:05 2017 : 10.70.6.202  admin    HTTP/1.1 DELETE  /rest/config/running/router/mpls1    400
Bad Request
Fri Sep 29 18:40:56 2017 : 10.70.6.202  admin    HTTP/1.1 GET  /rest/operational-state/mpls-state    200 OK
Fri Sep 29 18:41:22 2017 : 10.70.6.202  admin    HTTP/1.1 GET  /rest/    200 OK
Fri Sep 29 18:42:41 2017 : 10.70.6.202  admin    HTTP/1.1 POST  /rest/config/running/router/mpls/policy
<backup-retry-time>10</backup-retry-time>   200 OK
Fri Sep 29 18:46:27 2017 : 10.70.6.202  admin    HTTP/1.1 Uknown  /rest/config/running/router/mpls    405
Method Not Allowed
Fri Sep 29 19:00:32 2017 : 10.70.6.202  admin1    HTTP/1.1 DELETE  /rest/config/running/router/mpls/
policy    401 Unauthorized
Fri Sep 29 19:00:55 2017 : 10.70.6.202  admin    HTTP/1.1 POST  /rest/config/running/router/mpls/policy
<backup-retry-time>10</backup-retry-time>   500 Internal Server Error
```

Configuring SSH session rekey interval by volume and time

SSH servers can trigger rekeying once a certain time interval is reached or data traffic reaches a specified volume.

During rekeying, a set of key exchange messages are transferred between the SSH client and the server, changing the key used for the session security.

Rekeying by volume

In Common Criteria mode, the **rekey-volume** option cannot exceed a value equal to 1024 MB. The default value is 1024 MB.

The range of the rekey volume configured using the **ssh-server** command is 512 to 1024 MB.

```
device(config-rbridge-id-1)# ssh server rekey-volume ?
Possible completions:
  <DECIMAL>   <512-4095> Megabytes"
```

Rekeying by time

SSH rekey can also be configured based on time. The default value is 3600 seconds. The following command can be used to specify the time.

```
device(config-rbridge-id-1)# ssh server rekey-interval ?
Possible completions:
  <DECIMAL>   <900-3600> Seconds
```

Audit Logs

Certain operations will result in logging entries to the audit log. These entries are added to the log local to the device and are also sent to a syslog server if configured. The device maintains two local logs: auditlog and raslog. The entries related to starting and terminating connections as well as the configuration commands issued are logged in the auditlog while the rest of the entries are in raslog. The auditlog and raslog can contain up to 1000 entries and the oldest entries are removed as new ones are added when the maximum log size is reached.

All entries from both local logs are sent to the syslog server.

The entries follow the given format below:

Timestamp	Entry Number	Entry Type	Access Method	Device Name	Event	Event Description
2018/09/26-00:01:43 (GMT)	[SEC-3111]	INFO, SECURITY	NONE/root/NONE/None/CLI	sw0	Event: TLS SESSION	TLS handshake, Info: Successfully processed TLS connection . Host=134.141.41.168.

Where

Timestamp is when an event is recorded in the log
Entry Number is the item number in the log
Entry type is the type of the audit log item, in this example, an informational entry recorded by a security-related event
Access Method is how this event triggered and the access used for this event, the 5-tuple includes the user name, privilege and how the device is being accessed (e.g., CLI or none if through a protocol transition)
Device Name is the TOE
Event is the security-related trigger for this entry
Event Description contains additional information regarding the event

The log can be displayed from the CLI by

```
device# show logging auditlog
```

To display the latest logs and specify the number of entries to display, the following command can be used instead:

```
device# show logging auditlog reverse count 10
```

A list of relevant audit log entries are in Appendix A: Audit Log Entries

SYSLOG server configuration

The steps to configure a syslog server in the switch is described in the section Configuring Common Criteria mode.

This requires that a host or a device with the IP-address (our example above uses 10.20.238.120) specified in the configuration is reachable over the network and is running a SYSLOG server application.

That server application must be configured:

1. To accept connections over a secure channel using TLS, listening to a specified TCP port.
   The server TCP port is specified in the switch CLI configuration. Our example above uses port number 1999.
2. To use a server certificate signed by an intermediate CA using the CA-cert imported by the switch using the command '`crypto import syslogca`'.
3. To process the received syslog message, and this can be in various ways. For instance, user may save it to a local file, forward to another application or another host in the network.

Syslog client inactivity timeout uses the system default value of 132 minutes (2hrs and 12 minutes) which is based on the TCP keepalive mechanism. There is no support to modify this timeout value.

If the connection is lost the client will retry based on the TCP retransmission mechanism.

Appendix A: Audit Log Entries

The following table lists some of the notable log entries.

REST and TLS-related audit log entries

Operation	Log details
REST/TLS session establishment (server)	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Successfully processed TLS connection . Host=134.141.41.168.
REST/TLS session establishment (client)	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Establishing TLS connection: client 10.2.2.2.
REST/TLS session termination (client/server)	2018/09/26-00:01:46 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Terminating TLS connection. Host=134.141.41.168
Syslog (TLS) Client Termination	321 AUDIT,2018/12/08-02:14:54 (GMT), [SEC-3111], INFO, SECURITY, admin/admin/127.0.0.1/console/cli,, sw0, Event: TLS SESSION, TLS handshake, Info: Terminating connection to: 10.2.3.4:6514.
TLS Client Handshake failures (unable to connect)	321 AUDIT,2018/12/08-02:14:54 (GMT), [SEC-3111], INFO, SECURITY, admin/admin/127.0.0.1/console/cli,, sw0, Event: TLS SESSION, TLS handshake, Info: Handshake failure when connecting to server: 10.2.3.4.
REST/HTTPS authentication success	AUDIT,2018/10/09-13:57:20 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Successfully processed TLS connection . Host=134.141.41.162. AUDIT,2018/10/09-13:57:20 (GMT), [SEC-3020], INFO, SECURITY, admin/admin/134.141.41.162/http/REST Interface,, VDX6940-144S, Event: login, Status: success, Info: Successful login attempt via HTTP, IP Addr: 134.141.41.162.
HTTPS/REST access with invalid credentials	AUDIT,2018/10/09-13:54:10 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Successfully processed TLS connection . Host=134.141.41.162. AUDIT,2018/10/09-13:54:12 (GMT), [SEC-3021], INFO, SECURITY, admin/admin/134.141.41.162/http/REST Interface,, VDX6940-144S, Event: login, Status: failed, Info: Failed login attempt through HTTP, IP Addr: 134.141.41.162. AUDIT,2018/10/09-13:54:12 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Terminating TLS connection. Host=134.141.41.162.
Invalid TLS version (after this entry, the TLS Session Termination log is also displayed)	2018/09/12-02:11:13, [SEC-3110], 3695, SW/1 | Active, INFO, sw0, Event: TLS SESSION, TLS handshake failed with HTTPS client, Info: Wrong Protocol version number. Host=134.141.41.162.
Invalid TLS cipher (after this entry, the TLS Session Termination log is also displayed)	2018/09/12-02:11:14, [SEC-3110], 3696, SW/1 | Active, INFO, sw0, Event: TLS SESSION, TLS handshake failed with HTTPS client, Info: No matching cipher found. Host=134.141.41.162.
No matching cipher	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake failed, Info: No matching cipher found. Host=10.6.41.187.
Unsupported TLS version	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake failed, Info: Wrong Protocol version number. Host=10.6.41.187
Key exchange message of an invalid type	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Unknown key exchange type.
Decryption Failed or Bad Record MAC	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Decryption failed or bad record MAC.

Digest check failed	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Digest check failed.
Block cipher pad is wrong	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Block cipher pad is wrong.
Unexpected message (Finished message sent before the ChangeCipherSpec message)	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Bad change cipher spec.
Invalid server EKU being used	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info: unsupported certificate purpose.
Server selected a cipher suite not proposed by client	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake failed, Info: No matching cipher found. Host=10.24.12.86.
Unexpected message (Finished message sent before the ChangeCipherSpec message)	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Finished message sent before ChangeCipherSpec message.
Finished message is modified	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Finished message is modified.
Invalid server EKU being used/SSLv3 alert certificate unknown	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Certificates missing expected fields or invalid certificate.
Server negotiates unsupported cipher	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Server offered unsupported cipher.
No ciphers specified/ Server selects a ciphersuite not proposed by the client	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Server offered wrong cipher.
Unsupported TLS version offered by server	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Server offered unsupported SSL version.
Decryption failed or bad MAC/Finished message in plaintext	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3110], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: TLS SESSION, TLS handshake, Info: Decryption failed or bad record mac .

OCSP and Certificate-related Audit Log entries

Certificate contains OCSP URI, but device encountered error in parsing	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info: failed to parse OCSP responder url.
OCSP Responder is not reachable	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info: OCSP application verification failure.
Certificate status is unknown	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info: certificate is unknown for OCSP.
Certificate status if revoked	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info: certificate is revoked to OCSP.
OCSP responder is reachable but returns failure.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info: OCSP responder reports fail.

The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unable to get issuer certificate.
The certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value, this is only meaningful for RSA keys.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unable to decrypt certificate's signature.
The public key in the certificate SubjectPublicKeyInfo could not be read.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unable to decode issuer public key.
The signature of the certificate is invalid.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:certificate signature failure.
The certificate is not yet valid: the notBefore date is after the current time.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:certificate is not yet valid.
The certificate has expired: that is the notAfter date is before the current time.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:certificate has expired
The certificate notBefore field contains an invalid time.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:format error in certificate's notBefore field
The certificate notAfter field contains an invalid time.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:format error in certificate's notAfter field
The passed certificate is self signed and the same certificate cannot be found in the list of trusted certificates.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:self signed certificate
The certificate chain could be built up using the untrusted certificates but the root could not be found locally.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:self signed certificate in certificate chain
The issuer certificate of a locally looked up certificate could not be found. This normally means the list of trusted certificates is not complete.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unable to get local issuer
No signatures could be verified because the chain contains only one certificate and it is not self signed.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unable to verify the first certificate
The certificate chain length is greater than the supplied maximum depth.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:certificate chain too long
The certificate has been revoked.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:certificate revoked
A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:invalid CA certificate

The certificate is invalid. Either it is a CA or its extensions are not consistent with the supplied purpose.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:invalid non-CA certificate (has CA markings).
The basicConstraints path-length parameter has been exceeded.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:path length constraint exceeded
The supplied certificate cannot be used for the specified purpose.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unsupported certificate purpose
The root CA is not marked as trusted for the specified purpose.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:certificate not trusted.
The root CA is marked to reject the specified purpose.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:certificate rejected.
The current candidate issuer certificate was rejected because its keyUsage extension does not permit certificate signing. This is only set if issuer check debugging is enabled it is used for status notification and is **not** in itself an error.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:key usage does not include certificate signing
The certificate was rejected because its keyUsage extension does not include digital signature.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:key usage does not include digital signature
An unsupported name constraint type was encountered. OpenSSL currently only supports directory name, DNS name, email and URI types.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unsupported name constraint type.
The format of the name constraint is not recognised: for example an email address format of a form not mentioned in RFC3280. This could be caused by a garbage extension or some new feature not currently supported.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unsupported or invalid name constraint syntax.
The certificate common name doesn’t match with server hostname.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:Hostname mismatch.
	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:Hostname wildcard check failed.
The basicConstraints parameter is false for CA certificate.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:invalid CA certificate: basic constraints false for CA.
The basicConstraints parameter is absent for CA certificate.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:invalid CA certificate: basic constraints absent for CA.
	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:Email address mismatch.

The certificate common name doesn’t match with server’s IP address.	2018/09/26-00:01:43 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:IP address mismatch.

SSH related audit log entries

SSH key-exchange algorithms is changed	2018/10/08-17:44:27 (GMT), [DCM-1006], INFO, DCMCFG, admin/admin/134.141.54.182/console/cli,, VDX6940-144S, Event: database commit transaction, Status: Succeeded, User command: "configure config-rbridge-id-1 ssh server key-exchange diffie-hellman-group14-sha1". AUDIT,2018/10/08-17:44:27 (GMT), [SEC-3103], INFO, SECURITY, admin/admin/134.141.54.182/console/cli,, VDX6940-144S, Event: SSH Server, Status: success, Info: SSH Server Key Exchange is configured to diffie-hellman-group14-sha1
SSH server cipher is changed	2018/10/08-16:51:30 (GMT), [SEC-3079], INFO, SECURITY, admin/admin/134.141.54.182/console/cli,, VDX6940-144S, Event: SSH Server, Status: success, Info: SSH Server Cipher is configured to aes128-ctr.
SSH Failed login attempt	2018/10/08-16:50:18 (GMT), [SEC-3021], INFO, SECURITY, admin/admin/134.141.54.182/console/cli,, sw0, Event: login, Status: failed, Info: Failed login attempt through REMOTE, IP Addr: 134.141.41.152.
SSH Successful Login (Used by netconf as well)	2018/10/08-16:49:27 (GMT), [SEC-3020], INFO, SECURITY, admin/admin/134.141.41.152/ssh/CLI,, sw0, Event: login, Status: success, Info: Successful login attempt via REMOTE, IP Addr: 134.141.41.152.
SSH logout record/Inactivity timeout (Used by netconf as well)	2018/10/08-16:49:47 (GMT), [SEC-3022], INFO, SECURITY, admin/admin/134.141.54.182/ssh/cli,, sw0, Event: logout, Status: success, Info: Successful logout by user [admin].
Attempted connection with unsupported authentication algorithm	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3117], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: SSH SESSION, Invalid HostKey, Info: Peer sent an unsupported encryption algorithm list.
Attempted connection with unsupported authentication algorithm (no match)	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3117], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: SSH SESSION, Invalid HostKey, Info: The hostkey algorithm ssh_host_ed25519_key that matches with peer is not in supported list
Unsupported hash algorithm	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3117], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: SSH SESSION, Invalid Digest, Info: The hash algorithm sha1 is not in the supported list
Unsupported key exchange algorithm	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3117], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: SSH SESSION, Invalid Key Exchange, Info: Peer sent an unsupported key exchange algorithm list
Key exchange algorithm does not match	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3117], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: SSH SESSION, Invalid Key Exchange, Info: The key exchange algorithm curve25519-sha256@libssh.org that matches with peer is not in supported list
Oversized packet error	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3117], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: SSH SESSION, Packet Size Error, Info: Failed to process packet, size 2700 is above limit 1960.
Unsupported encryption algorithm	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3117], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: SSH SESSION, Invalid Cipher, Info: Peer sent an unsupported encryption algorithm list
Encryption algorithm does not match	1017 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3117], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: SSH SESSION, Invalid Cipher, Info: The encryption algorithm chacha20-poly1305@openssh.com that matches with peer is not in supported list
Unsupported MAC integrity algorithm	1021 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3118], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: SSH SESSION, Invalid Mac, Info: Peer sent an unsupported mac

	list.
	1021 AUDIT,2018/09/26-00:01:43 (GMT), [SEC-3118], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: SSH SESSION, Invalid Mac, Info: The mac algorithm umac-128@openssh.com that matches with peer is not in supported list

Miscellaneous Entries

User is locked out once certain number of retries with invalid credentials is reached	Account locked - maximum login failure threshold reached. **(Displayed on the console)** 2018/09/26-00:26:30, [SEC-1192], 4249, SW/1 | Active, INFO, sw0, Security violation: Login failure attempt via SERIAL.
FIPS self-tests are enabled	AUDIT,2018/10/09-21:12:04 (GMT), [SEC-3046], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, The FIPS Self Tests mode has been set to Enabled/None.
Changing the date and time from the CLI	AUDIT,2018/10/09-21:31:06 (GMT), [TS-1009], INFO, SECURITY, admin/admin/134.141.54.182/console/cli,, VDX6940-144S, Event: change time: attempt. AUDIT,2018/10/09-21:31:06 (GMT), [TS-1010], INFO, SECURITY, admin/admin/134.141.54.182/console/cli,, VDX6940-144S, Event: change time: success, Info: from 2018-10-09 21:31:06 to 2018-10-09 13:34:00.

Firmware update/download audit log entries

Firmware download command has been started	AUDIT,2018/10/10-20:49:06 (GMT), [SULB-1000], WARNING, FIRMWARE, admin/admin/127.0.0.1/console/cli,, VDX6740T, The firmware download command has been started.
Firmware install begins	AUDIT,2018/10/10-20:49:12 (GMT), [SULB-1100], INFO, FIRMWARE, NONE/root/NONE/None/CLI,, VDX6740T, Firmware install begins on SW/0. AUDIT,2018/10/10-20:53:31 (GMT), [SULB-1100], INFO, FIRMWARE, NONE/root/NONE/None/CLI,, VDX6740T, Firmware install begins on SW/1.
Firmware install ends	AUDIT,2018/10/10-20:53:30 (GMT), [SULB-1101], INFO, FIRMWARE, NONE/root/NONE/None/CLI,, VDX6740T, Firmware install ends on SW/0. AUDIT,2018/10/10-20:56:18 (GMT), [SULB-1101], INFO, FIRMWARE, NONE/root/NONE/None/CLI,, VDX6740T, Firmware install ends on SW/1.

Console login audit log entries

Successful login	AUDIT,2018/11/09-15:45:55 (GMT), [SEC-3020], INFO, SECURITY, admin/admin/NONE/console/CLI,, sw0, Event: login, Status: success, Info: Successful login attempt via SERIAL.
Failed login	AUDIT,2018/11/09-15:46:59 (GMT), [SEC-3021], INFO, SECURITY, admin/NONE/NONE/None/CLI,, sw0, Event: login, Status: failed, Info: Failed login attempt through SERIAL.
Logout	AUDIT,2018/11/09-15:46:54 (GMT), [SEC-3022], INFO, SECURITY, admin/admin/NONE/console/CLI,, sw0, Event: logout, Status: success, Info: Successful logout by user [admin].

Firmware download completed successfully	AUDIT,2018/10/10-21:12:15 (GMT), [SULB-1103], INFO, FIRMWARE, NONE/root/NONE/None/CLI,, VDX6740T, Firmware download completed successfully on SW/1. AUDIT,2018/10/10-21:12:15 (GMT), [SULB-1103], INFO, FIRMWARE, NONE/root/NONE/None/CLI,, VDX6740T, Firmware download completed successfully on SW/0.
Firmware upgrade session completes.	AUDIT,2018/10/10-21:12:15 (GMT), [SULB-1106], WARNING, FIRMWARE, NONE/root/NONE/None/CLI,, VDX6740T, Firmware upgrade session (0: dual-MM upgrade continue) completes.
Firmware install failed. Due to files failing signature check error (62)	AUDIT,2018/10/10-21:42:28 (GMT), [SULB-1102], WARNING, FIRMWARE, NONE/root/NONE/None/CLI,, VDX6740T, Firmware install failed on SW/0 with error (62).
Firmware recover begins. Recovering from error (62)	AUDIT,2018/10/10-21:42:28 (GMT), [SULB-1100], INFO, FIRMWARE, NONE/root/NONE/None/CLI,, VDX6740T, Firmware recover begins on SW/0.
Firmware recover ends. Recovery completes	AUDIT,2018/10/10-21:42:38 (GMT), [SULB-1101], INFO, FIRMWARE, NONE/root/NONE/None/CLI,, VDX6740T, Firmware recover ends on SW/0.
Firmware download failed but recovered from error (62)	AUDIT,2018/10/10-21:42:39 (GMT), [SULB-1104], CRITICAL, FIRMWARE, NONE/root/NONE/None/CLI,, VDX6740T, Firmware download failed but recovered on SW/0 with error (62).

Self -Test Messages from the Console

These are the messages displayed in the console during self-tests at startup:

```
       FIPS-mode test application

1. Non-Approved cryptographic operation test...
       a. Excluded algorithm (MD5)...successful
       b. Included algorithm (D-H)...successful
2. Automatic power-up self test...
       2.a. FIPS RNG (AES_256_CTR_DRBG) selftest...successful
3. AES-128 CBC  encryption/decryption...successful
4. RSA key generation and encryption/decryption...successful
4.1. RSA 2048 with 'SHA256' testing...successful
5. TDES-CBC encryption/decryption...successful
6a. SHA-1 hash...successful
6b. SHA-256 hash...successful
6c. SHA-384 hash...successful
6d. SHA-512 hash...successful
6e. HMAC-SHA-1 hash...successful
6f. HMAC-SHA-224 hash...successful
6g. HMAC-SHA-256 hash...successful
6h. HMAC-SHA-384 hash...successful
6i. HMAC-SHA-512 hash...successful
7. Non-Approved cryptographic operation test...
       a. Excluded algorithm (MD5)...Not executed
       b. Included algorithm (D-H)...successful as expected
8. Zero-ization...Successful
9. TLS KDF 1.0...successful
9a. TLS KDF 1.2...successful
10.ECDSA ...successful
11.ECDH ...successful
All tests completed with 0 errors
```

When failure is observed by each test, the device displays a message for the algorithm that failed and the box reboots. An example is shown below:

```
running /usr/bin/fips_test_suite aes...
       FIPS-mode test application

AES-128 CBC encryption/decryption with corrupted KAT... FAILED as EXPECTED!
Power-up self test with corrupted KAT failed!
Rebooting ...
```