CONFIGURATION GUIDE

Extreme SLX-OS Common Criteria Configuration Guide, 20.2.1aa

Supporting SLX-OS 20.2.1aa

Version 2.5.2
7 July 2021

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Preface

This section describes the text conventions used in this document, where you can find additional information, and how you can provide feedback to us.

Conventions

This section discusses the conventions used in this guide.

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.

Format	Description
`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.

Documentation and Training

Find Extreme Networks product information at the following locations:

- Current Product Documentation
- Release Notes
- Hardware/software compatibility matrices for Campus and Edge products
- Supported transceivers and cables for Data Center products
- Other resources, like white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

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

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: (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

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

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- 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

Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form (all fields are required).
3. Select the products for which you would like to receive notifications.

   NOTE
   You can modify your product selections or unsubscribe at any time.

4. Select **Submit**.

Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@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.

About This Document

What's new in this document

The SLX-OS 20.2.1aa software release is the first SLX release for Common Criteria certification.

The following table includes descriptions of new information added to this guide for the SLX-OS 20.2.1 software release.

TABLE 1 Summary of enhancements in the SLX-OS <<< release

Version	Summary of Changes	Date
1.0	Initial Release	February 2021

For complete information on this SLX-OS software release, refer to the *SLX-OS 20.2.1 Release Notes*.

Supported Hardware

For instances in which a topic or part of a topic applies to some devices but not to others, the topic specifically identifies the devices.

SLX-OS 20.2.1aa supports the following hardware platforms.

- Devices based on the Broadcom DNX® chipset family:
  - ExtremeSwitching SLX 9540
  - ExtremeRouting SLX 9740

  NOTE
  Although many software and hardware configurations are tested and supported for this release, documenting all possible configurations and scenarios is beyond the scope of this document.

For information about other releases, see the documentation for those releases.

Common Criteria Certification

Common Criteria Overview

Common Criteria (CC) certification for a device enforces a set of security standards and limits features to comply with the CC standards, similar to placing the FIPS mode device. For information about security functions subject to certification, see *Extreme Networks, Inc. SLX Product Series operating with version 20.2.1aa (NDcPP2.2e) Security Target*.

Common Criteria compliance supports Extreme SLX-OS devices running 20.2.1aa. Cryptographic Algorithm Validation System (CAVS) certifies all cryptographic algorithms required and used in CC. The RNG component does not require configuration and follows the specified requirements as above.

The sections that follow contain steps to configure the Extreme Networks SLX-OS switch for Common Criteria standards with SLX-OS version 20.2.1aa collaborative Protection Profile for Network Devices (NDcPP) version 2.2e.

Establish a Serial Connection

Use a serial connection from a workstation or terminal to do the configuration tasks. Connect the serial port to a workstation to configure the device's IP address before connecting it to a fabric or IP network.

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

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.

The location of the serial port is on the port side of the chassis. The Extreme device uses an RJ-45 connector or a mini-USB connector for the serial port. Provided with each model is an RJ-45 to DB9 adapter, and the cable supplied is a rollover cable. Refer to the Technical Specifications for a listing of serial cable pinouts.

Create a serial connection to the device:

1. Connect the serial cable to the serial port on the device and an RS-232 serial port on the workstation or terminal device.

   NOTE
   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:
   a) In a Windows environment, enter the following values: 9600 bits per second, 8 data bits, no parity, stop bit, and no flow control.
   b) In a UNIX environment using TIP, enter: `tip /dev/ttyb -9600`. If ttyb is already in use, use ttya instead.

Serial Port Specifications

Pinout Mini-USB

Pin Signal Description

- +5V Not used
- UART0_Tex Debug port
- UART0_RX Console port
- IN Not used
- GND Ground

Pinout RJ-45

Pin Signal Description

- Not supported N/A
- Not supported N/A
- UART1_RXD Receive data
- GND Logic ground
- GND Logic ground
- UART1_TXD Transmit data
- Not support N/A
- Not support N/A

Protocol

Parameter value

- Baud 9600
- Data bits 8
- Parity None
- Stop bits 1
- Flow control None

Set the Management IP Address

Once the device is accessible through a serial interface, configure the management interface's IP address so you can perform various network functions. Use the **configure terminal** command and provide either a static IP address or the **dhcp** keyword. The interface's IP address can be removed using the `no` form of the **ip address** command.

```
device# configure terminal
device# interface Management 0
device(config-Management-0)# ip address [10.24.12.139/22 || dhcp]
```

Access the Device

An SLX device can be accessed or managed using various options. These include console access (over serial interface), SSH, REST requests, and NETCONF requests. The serial connection is described in Establish a Serial Connection on page 11.

Access the device using SSH from a remote client:

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

Provide the appropriate user credentials to gain access to the device. Close the session with the CLI **exit** command.

Example:

Send and receive NETCONF request to the device, specify the NETCONF port as in this example:

```
remote-device-prompt# ssh admin@10.24.12.515 -p 830 -s netconf
```

NOTE

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

After you configure the HTTPS server, you can send an HTTPS request with appropriate user credentials. If the credentials are valid, the HTTPS server provides a reply over the secure channel.

The device, by default, has 'admin' and 'user' for access. Create custom users using the **SLX(config)# username** command. Device access is denied based on the password attribute lockout configuration for Console, SSH, REST, and NETCONF requests. For more information, see Configure Password Criteria, Admins, and Permissions on page 16.

NOTE

Even if password attribute lockout configuration is enabled, admin users can access the device using the console but not with SSH, REST, and NETCONF requests. The administrator logins over the serial port/console are never locked out. Close the console (local) and remote network connections by issuing either exit or logout from the command prompt.

Common Criteria Preparation Overview

A user with administrative privileges can only perform the steps to configure the TOE to support Common Criteria requirements. 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. Automatically block and/or disable unsupported port and protocols.
9. Configure ACLs to block unused protocol ports and allow ports for supported protocols.
10. For authentication by RADIUS server(s) over TLS, import the RADIUS server's CA certificate.
11. To support TLS for Syslog, import the CA certificate of the Syslog server.
12. To support SSH public-key authentication, import the external client public key. See Configure SSH Authentication section below.
13. To enable x.509v3 certificate-based authentication with SSH, please follow the steps described in Appendix B: X.509v3 SSH Authentication on page 43.

Configuring Common Compliance 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. Before configuring the CC compliance mode, you must block the NETCONF interface.

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

```
device# unhide fips
```

You have access to all FIPS commands, such as the **fips zeroize** command.

3. Enter the **fips cc-enable** command to move the crypto module to Common Criteria mode, which triggers the algorithm self-tests and erase configuration databases except as noted. The TOE reboots afterward.

```
device#fips cc-enable
This command enables CC mode on this device and entails,
1. Erasing all passwords, shared secrets, private keys, entire
   configuration database (except mgmt IP and licenses) and then reloading the switch.

2. Once in CC mode (after reload), the system disables the following services or commands.
    a) Telnet server is disabled and the corresponding config commands are blocked.
    b) Telnet client CLI is blocked.
    c) HTTP server is disabled. HTTPS server can be used instead.
    d) HTTP client is not available for operations like, Firmware download.
    e) TFTP client cannot be used in copy commands.

3. The following services are not recommended to be enabled in CC mode.
    i) SNMP v1, v2c and v3.
    ii) TACACS+
   iii) LDAP
    iv) For recommended SSH algorithms in CC mode, please refer to the help string of SSH server
cipher, SSH server key-exchange
        and SSH server mac CLI commands.

Do you want to continue? (yes, y, no, n) [no]:y
```

At this point, only CC allowed algorithms are operational. Administrators can manage keys that will be used for certificates or for an SSH host key. These keys can be generated and deleted using commands defined in sections “Configure SSH”, “Configure the HTTPS Server” and “Appendix B: X.509v3 SSH Authentication.” Trusted CA certificates can also be imported or deleted using instructions found in these same sections as well as sections for the configuration of Radius and Syslog.

Trusted Root Certificates

Trusted root certificates for applications syslog, RADIUS, and SSH x509 can be imported to the device and removed via their corresponding `no` forms.

```
no | crypto import syslogca | radiusca | sshx509v3ca host <hostip> user <username> password <password>
directory <dir name> file < ca file> protocol scp|ftp
```

To view imported certificates, use the following command:

```
show crypto ca certificates
```

Configure Crypto Compliance

Configure the system for crypto compliance.

1. Enter into the global configuration mode.

```
device# configure terminal
```

2. Configure the host name.

```
device(config)# switch-attributes host-name <Host name>
```

3. Configure a domain name.

```
device(config)# ip dns domain-name <Domain name>
```

4. Configure the external DNS servers.

```
device(config)# ip dns name-server <IP address> use-vrf mgmt-vrf
```

5. Show the DNS configuration.

```
device(config)# do show running-config ip dns
device(config)# do show ip dns
```

6. Verify the DNS resolution.

```
device(config)# do ping <host name> vrf mgmt-vrf
```

7. Configure the external NTP servers in secure mode using the following steps.

NOTE
You can configure a maximum number of eight NTP servers.

a) Configure the NTP keys for Authentication.

```
device(config)# ntp authentication-key <key-id> <Auth-Type: sha1> <Auth-Secret> encryption-level
7
```

NOTE
Use only the SHA1 parameter for the auth-type.

b) Configure an external server.

```
device(config)# ntp server <IP address> key <key-id> version <version no>
```

c) Show the NTP configuration.

```
device(config)# do show running-config ntp
```

d) Show the NTP sync status.

```
device(config)# do show ntp status
device(config)# do show ntp association
```

NOTE
Administrators cannot enable multicast or broadcast time updates via any CLI.

Configure Password Criteria, Admins, and Permissions

Enable strict password checking by issuing the following commands.

```
device(config)# password-attributes min-length
# min-length can be configured between 8 and 32. The administrator should set the value to at least 15
characters.
device(config)# password-attributes max-retry
# max-retry can be configured between 0 and 16. The administrator should set the value to at least 3
retries.
device(config)# password-attributes max-lockout-duration
# max-lockout-duration can be configured between 0 and 99999 minutes. The administrator should set the
value to at least 5 minutes.
device(config)# password-attributes admin-lockout
# admin-lockout can be Enabled/Disabled. The administrator should set this value to enabled.
```

Configure SSH

Configure the secure shell (SSH) elements.

1. Remove the SSH RSA host key.

```
device(config)# no ssh server key dsa
```

2. If the ECDSA host key is not required, remove it.

```
device(config)# no ssh server key ecdsa 256
```

3. Configure the SSH server key-exchange protocol.

```
device(config)# ssh server key-exchange diffie-hellman-group-14-sha1
```

4. Configure the SSH server cipher & MAC algorithms.

```
device(config)# ssh server cipher aes128-ctr, aes256-ctr, aes128-cbc, aes256-cbc
device(config)# ssh server mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
```

5. Set the timeout value for SSH connections to the server. This setting affects SSH connections to the server, including the netconf sessions.

```
device(config)# ssh server max-idle-timeout 20
device(config)# line vty exec-timeout 100

This command affects both the SSH CLI connection and the serial console connection.
```

6. Set the number of login attempts.

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

7. Sset the login timeout. Set the value to an appropriate timeout period in the administrator's environment.

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

8. Configure SSH server rekey volume and rekey interval.

```
device(config)# ssh server rekey-volume <Megabytes: 512-4095 (default: 1024 MB)>
device(config)# ssh server rekey-interval <Seconds: 900-3600 (default: 3600)>
```

NOTE
The rekey interval must be less than 1 hour in CC mode, and rekey volume must be less than 1 GB.

9. Restart the SSH server. Any changes to ssh-server require a restart as the SSH server cannot be restarted by itself.

```
device(config)# do ssh-server restart
device(config)# do show ssh server status
```

Configure the HTTPS Server

The SLX in FIPS CC mode only allows use of RSA 2048-bit keys, as well as ECDSA keys with curves P-256, P-384 or P-521 when in FIPS CC mode. The system enforces it, and if an administrator configures anything else, they receive an error and configuration failure. It is necessary to comply with the Common Criteria validated mode of operation. No special configuration is required for SLX to support session resumption using session tickets.

1. Generate a key pair to sign and encrypt the security payload during the security protocol exchanges.

```
device(config)# crypto key label <trust1> (ecdsa|rsa) modulus <Decimal:ecdsa 256|384|521 || rsa 2048>
```

2. Configure a trusted Certificate Authority (CA) to verify the imported identity certificate issued by one of the locally trusted CAs.

```
device(config)# crypto ca trustpoint <trust1>
```

3. Associate the key pair to the trust point. The association between the trust point, key pair, and identity certificate are valid until it is explicitly removed by deleting the certificate, key pair, or trust point.

```
device(config-ca-t1)# keypair <trust1>
device(config-ca-t1)# exit
```

4. Authenticate the device to the CA by obtaining the CA's certificate. Contact the CA administrator to authenticate the CA public key by comparing the fingerprint of the CA certificate.

```
device# crypto ca authenticate <trust1> cert-type https protocol SCP host <IP Address> directory <dir> file
<ca file> user <user name> password <password>
```

5. Export the enrollment certificate to the location specified for the remote host.

```
device# crypto ca enroll <trust1> cert-type https protocol SCP country <US> state <CA> locality <San
Jose> organization <Engg> orgunit <Engg> common <jdoe> directory <dir> host <IP address> user <user
name> password <password>
```

6. Generate an identity certificate at the trusted CA using the CSR sent in the previous step.

```
</root/jdoe/certs> # openssl ca -policy policy_strict -extensions server_cert -out jdoe.pem -
config ../openssl.cnf -infiles https.csr
```

7. Import and install the identity certificate from the trust point CA.

```
/root/jdoe/certs file jdoe.pem host 10.24.15.200<IP Address> user root<user name> password
pass<password>
```

8. Restart the HTTP server for the imported certificate to take effect.

```
device(config)# http server use-vrf mgmt-vrf shutdown
device(config)# http server use-vrf default-vrf shutdown
device(config)# no http server use-vrf mgmt-vrf shutdown
device(config)# no http server use-vrf default-vrf shutdown
```

Block Internal Ports

Use IP ACLs to block Extreme Networks internal ports 9110, and 9710 for IPv4 and IPv6.

Use IP ACLs to block Extreme Networks internal ports 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 RADIUS, enter **seq permit** commands to allow UDP and TCP traffic on ports 1024 through 65535.
- Configure IP ACLs using **ip access-list** command and use **ip access-group** command to apply the rules to the management interface.

Example:

```
device(config)# ip access-list extended <User defined name (i.e.FIPS-ACL4)>
device(config-ip-ext)# seq 1 deny tcp any any eq 9110
device(config-ip-ext)# seq 2 deny tcp any any eq 9710
device(config-ip-ext)# seq 3 permit tcp any any range 1024 65535
device(config-ip-ext)# seq 4 permit udp any any range 1024 65535
device(config-ip-ext)# seq 5 permit tcp any any eq 22
device(config-ip-ext)# seq 6 permit udp any any eq 123
device(config-ip-ext)# seq 7 permit tcp any any eq 443
device(config-ip-ext)# seq 8 permit tcp any any eq 830
device(config-ip-ext)# exit
device(config)# interface Management <ID for Management Interface (i.e. 0)>
device(config-Management-0)# ip access-group <User defined name (i.e.FIPS-ACL4)>in

device(config)# ipv6 access-list extended <User defined name (i.e.FIPS-ACL6)>
device(config-ip-ext)# seq 1 deny tcp any any eq 9110
device(config-ip-ext)# seq 2 deny tcp any any eq 9710
device(config-ip-ext)# seq 3 permit tcp any any range 1024 65535
device(config-ip-ext)# seq 4 permit udp any any range 1024 65535
device(config-ip-ext)# seq 5 permit tcp any any eq 22
device(config-ip-ext)# seq 6 permit udp any any eq 123
device(config-ip-ext)# seq 7 permit tcp any any eq 443
device(config-ip-ext)# seq 8 permit tcp any any eq 830
device(config-ip-ext)# exit
device(config)# interface Management <ID for Management Interface (i.e. 0)>
device(conf-Management-0)# ipv6 access-group <User defined name (i.e.FIPS-ACL6)>in
```

NOTE

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

Configure the RADIUS Server

Configure the RADIUS server to enable authentication.

1. Import the RADIUS server CA certificate:

   NOTE

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

   ```
   device# crypto import radiusca protocol SCP host <IP address> directory <dir> file <ca cert> user
   <user name> password <password>
   ```

2. Show the imported certificates:

   ```
   device# show crypto ca certificates
   ```

3. Delete the imported certificate, if required:

```
device# no|crypto import radiusca
```

4. Configure TLS ciphers for RADIUS authentication:

```
device# cipherset RADIUS
```

5. Configure the RADIUS server:

```
device(config)# radius-server host <IP-address|Hostname> [use-vrf <VRF-name>] [auth-port <portnum>]
[radsec] [timeout <secs>] [retries <num>] [key <shared secret for encryption>] [protocol <chap|pap|
peap>] [encryption-level <0 | 7>]

device(config)# radius-server host <server IP Address> use-vrf mgmt-vrf ?
Possible completions:
  auth-port  Port used for Authentication
     (default=1812 for RADIUS/UDP, 2083 for RADIUS/TLS)
  radsec     RADIUS/TLS protocol should be used instead of RADIUS/UDP
  protocol   Authentication protocol to be used (default=CHAP)
  encryption-level   Level of encryption of the key (default=7)
  key        Secret shared with this server
          (default='sharedsecret' for RADIUS/UDP, 'radsec' for RADIUS/TLS)
  retries    Number of retries for this server connection (default=5)
  timeout    Wait time for this server to respond (default=5 sec)
```

The device enforces certificate validation during import, as described in TLS Server Certificate Authentication on page 27.

6. Configure RADIUS as the primary authentication method and “local” as the secondary authentication method:

```
device(config)# aaa authentication login radius local-auth-fallback
```

Enable Secure Logging

Enable secure logging using the Syslog server.

1. Import the Syslog server CA certificate in privileged EXEC mode.

```
device# crypto import syslogca protocol SCP host <IP address> directory <dir> file <ca file> user
<user name> password <password>
```

2. Show the imported certificates:

```
device# show crypto ca certificates
```

3. Delete the imported certificate, if required:

```
device# no|crypto import syslogca
```

4. Configure the Syslog server.

```
device(config)# logging syslog-server <IP address> | use-vrf <vrf>
device (config)# secure port <port:1-65535[6514]>
```

Alternatively configure the syslog server by hostname.

We are introducing a new CLI option to enable configuration of DNS hostname to syslog server.

```
device(config)# logging syslog-server-host <hostname> | use-vrf <vrf>
device (config)# secure port <port:1-65535[6514]>
```

To configure the syslog hostname user must have the DNS server and the domain name configured as below.

SLX(config)#ip dns name-server <DNS server IP>

SLX(config)#ip dns domain-name <hostname>

If the configured DNS server is able to resolve the syslog hostname then only the CLI configuration will be successful. Due to the resolution happening during the config at 2 levels according to design, the syslog-server-host CLI command will take few seconds to execute.
If the DNS resolution fails user will get below error and CLI configuration will fail.

SLX(config)# logging syslog-server-host abcd
% Error: The configured syslog hostname could not be resolved. Please check if DNS server is configured or reachable or check the DNS server configurations.

When the DNS field in the syslog server certificate SAN mismatches with the configured hostname user will get below raslog

```
SLX(conf-if-eth-0/2)# 2021/04/14-18:22:25, [SEC-3112], 373,, INFO, SLX, Event: X509v3, Certificate
Validation failed, Info: Reason = Certificate subject alternative name does not match hostname
Certificate Details = [Subject CN EMIS Intermediate CA,
Serial 4097 Issuer /C=US/ST=California/O=ExtrNet Inc/OU=DCIP EMIS Certificate Authority/CN=EMIS
Intermediate CA].
```

When the DNS field in the syslog server certificate CN mismatches with the configured hostname user will get below raslog

```
SLX(conf-if-eth-0/2)# 2021/04/14-19:07:04, [SEC-3112], 386,, INFO, SLX, Event: X509v3, Certificate
Validation failed, Info: Reason = Common name does not match host IP
Certificate Details = [Subject CN rh107.emis.lab.1000,
Serial 4101 Issuer /C=IN/ST=KAR/O=EXTREME/OU=EMIS/CN=Intermediate Sub
CA/emailAddress=syslogPOC@extremenetworks.com].
```

Limitations :

- When using DNS only one syslog server may be specified.
- After upgrade the user has to remove the configured syslog-server-host and IP DNS server and reconfigure it to make the syslog hostname work.
- Syslog client inactivity timeout uses the system default value of 132 minutes (2 hrs 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.

5. On the configured port, run the OCSP responder.

```
openssl s_server -accept <secure-port> -CAfile <intermediate-certificate> -cert <server-certificate>
-key <server-certificate-key> -cipher <supported-cipher> -msg
```

NOTE

You can use IPv4 and IPv6 addresses when configuring the Syslog and RADIUS servers. These IPV4 or IPV6 addresses must be present as the common name (CN) or subject alternate name (SAN) in the TLS server certificate used for TLS connection. SAN takes precedence when present over CN. Both SAN and CN support IP addresses, and DNS hostname. The presence of wildcards in the IP addresses is also not accepted, and the connection gets dropped in this case.

Configure SSH Authentication

Import the public key to the TOE using the **certutil import sshkey directory** *pubkey-directory* **file** *filename* **protocol SCP host** *remote-ip* **user** *user-account password password* command. The term user indicates a valid user configured on the SLX with a user or administrator role.

1. Generate the key pairs externally using RSA-2048.
2. Import an SSH public key for a local SSH user from a remote host using the login credentials and pathname.

```
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'.
```

3. Enable x.509v3 based SSH authentication. For more information, see the steps described in Appendix B: X.509v3 SSH Authentication on page 43.
4. In global configuration mode, disable the Telnet server:

```
device(config)# telnet server shutdown
```

Configure the Banner Message

The banner message that provides information to the user when the TOE is accessed. The “Banner login” feature was evaluated as part of the Common Criteria certification. The other features, while allowed, were not tested. At a minimum, “Banner login” should be used to ensure a banner message is displayed on the console and via SSH access to the SLX platform.

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

```
device(config)# banner motd <message>
device(config)# no banner motd
device(config)# banner incoming <message>
device(config)# no banner incoming
device(config)# banner login <message>
device(config)# no banner login
```

- **banner motd** - Banner text displayed before the user logs into the switch.
- **banner incoming** - Banner text displayed on Console when the user is logged into Console.
- **banner login** – Sets the switch banner and the message is displayed on the logged in session after the user is authenticated.

2. 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
```

Download and Update the Firmware

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. Extreme uploads the signed firmware as a tar file with its associated SHA256 on a secure location.

   NOTE
   File location and version details are provided.

2. Download and verify with the downloaded image with a SHA256 checksum utility.
3. The digital signatures of various packages are downloaded first and used for package validation.
4. As part of the firmware download, verifying the signature validates each package in which there is no way to see the validated files visibly. The TOE does this process without administrator intervention. The installation fails if a file cannot be verified:

```
 "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."
```

5. Installation begins after the packages are validated.
6. By default, when the firmware downloads to the system, it reboots the system and commits the firmware automatically. When installing the firmware, the device reboots, and the administrator must wait until the device reports that the CLI can accept commands. Also, device functions are affected until the device reports that the firmware upgrade completes successfully. Delayed firmware activation is not supported.

   Firmware download

   Syntax:

```
device# firmware download {default-config | fullinstall | ftp | http | scp | sftp | usb |
interactive} [manual | coldboot] host {hostname | host_ip_address} user <username> password
<password> directory <directory> [file <Package release file, example:release.plist>] use-vrf <vrf
name, example: mgmt-vrf>
```

   Example:

```
device# firmware download scp coldboot user admin file release.plist directory /slx20.1.1aa/dist
host 10.1.2.3
```

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

   Parameters:

   default-config

   Sets the configuration back to default except for the following parameters:

Management IP and gateway. These two parameters are retained except when specifying the options to change their values.

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 and prompts you 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 management modules, resulting in a full reboot of the unit.

host:

Specifies the host by DNS name or IP address.

Hostname:

Specifies an IPv4 DNS hostname.

host_ip_address:

Specifies the host IP address. IPv4 and IPv6 addresses are supported.

Directory:

Provides a path to the '…./dist' folder on the remote server where the SLX image is available for download.

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

The publickey 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 using the **firmware download** command. When downloading new firmware, it always replaces the public key file on the switch with the new firmware, allowing you to have planned firmware key changes.

You can download the signed firmware with its associated SHA256 from www.extremenetworks.com.

The firmware package's digital signature is the definitive method to determine its validity during download and installation.

Update the Firmware

1. The digital signatures of various packages are downloaded first and used for package validation.

2. As part of the firmware download, verifying the signature validates each package in which there is no way to see the validated files visibly. The TOE does this process without administrator intervention. The installation fails if a file cannot be verified:

```
 "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, when the firmware downloads to the system, it reboots the system and commits the firmware automatically. When installing the firmware, the device reboots, and the administrator must wait until the device reports that the CLI can accept commands. Also, device functions are affected until the device reports that the firmware upgrade completes successfully. Delayed firmware activation is not supported.

   Firmware download

   Syntax:

```
device# firmware download {default-config | fullinstall | ftp | http | scp | sftp | usb |
interactive} [manual | coldboot] host {hostname | host_ip_address} user <username> password
<password> directory <directory> [file <Package release file, example:release.plist>] use-vrf <vrf
name, example: mgmt-vrf>
```

   Example:

```
device# firmware download scp coldboot user admin file release.plist directory /slx20.1.1aa/dist
host 10.1.2.3
```

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

   Parameters:

   default-config

   Sets the configuration back to default except for the following parameters:

   Management IP and gateway. These two parameters are retained except when specifying the options to change their values.

   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 and prompts you 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 management modules, resulting in a full reboot of the unit.

   host:

Specifies the host by DNS name or IP address.

Hostname:

Specifies an IPv4 DNS hostname.

host_ip_address:

Specifies the host IP address. IPv4 and IPv6 addresses are supported.

Directory:

Provides a path to the '…./dist' folder on the remote server where the SLX image is available for download.

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

The publickey 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 using the **firmware download** command. When downloading new firmware, it always replaces the public key file on the switch with the new firmware, allowing you to have planned firmware key changes.

You can download the signed firmware with its associated SHA256 from www.extremenetworks.com.

The firmware package's digital signature is the definitive method to determine its validity during download and installation.

View the Installed Firmware Version

View the installed firmware version:

```
device# show version
SLX-OS Operating System Version: 20.2.1
Copyright (c) 1995-2020 Extreme Networks, Inc.
Firmware name:      20.2.1aa
Build Time:         01:01:58 Mar 18, 2020
Install Time:       09:44:09 Jun 17, 2020
Kernel:             4.14.67
Control Processor: Intel(R) Atom(TM) CPU C3758 @ 2.20GHz, 8 cores
Microcode Version:  0x2e
Memory Size:        System Total: 15632 MB
System Uptime:      0days 0hrs 16mins 57secs

Name     Primary/Secondary Versions
------------------------------------------------------------
SLX-OS   20.2.1aa
         20.2.1aa
```

Display the crypto library information:

```
device# show fips
```

Password Requirements

You can configure password attributes to include the minimum length, character sets, and the number of retries. You can also set the length of time an account can be locked out when the maximum number of login failures occur.

Our recommendation: The 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.

> **NOTE**
> SLX allows special characters as part of the passwords. The following characters are allowed in a user or administrator password in the SLX system. `!@#$%^&*()_+=-`~`

The commands to configure password attributes are listed below.
password-attributes min-length

Specifies the minimum length of the password. Valid values range from 8 through 32 characters. The default is eight characters and does not need to be enabled to enforce an eight-character password length minimum.

```
device(config)# password-attributes min-length {8-32 default=8}
```

> **NOTE**
> Longer passwords are more robust, so set the minimum length to a value appropriate for the environment's threats.

password-attributes max-retry

Specifies the number of failed password logins permitted before a user is locked out. Values range from 0 through 16 attempted logins. The default value is 0. This value must be set.

```
device(config)# password-attributes max-retry 4
```

password-attributes max-lockout-duration

Specifies the maximum number of minutes after which the user account is unlocked. The range is from 0 through 99999. The default is 0, representing an infinite duration.

```
device(config)# password-attributes max-lockout-duration 10
```

Set the System Date and Time

Manually set the system date and time:
device# clock set CCYY-MM-DDTHH:MM:SS

where

CCYY-MM-DDTHH:MM:SS

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

REST APIUsage

REST is an administrative interface available for remotely managing SLX.

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

Enable the HTTPS server as described in Configuring Common Compliance Mode on page 14.

Start the HTTPS server:

```
config#http server use-vrf <vrf-name> shutdown
config#no http server use-vrf <vrf-name> shutdown
```

NOTE
vrf-name is like *mgmt-vrf*, *default-vrf* and is based on which vrf the interface is physically connected to when configured.

Once the HTTPS server is configured, an HTTPS request with the user credentials is sent to the server. If the credentials are valid, the HTTPs server provides 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 an IP address 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.

If the TLS server certificate validation fails during the TLS handshake, users are notified using Raslog/Auditlog with a reason.

TLS Cipher Suites for Client and Server Applications

You cannot use the command line to change the TLS cipher suites by the TOE's client and server applications because they are preset. The SLX in FIPS CC mode only accepts TLS v1.2 and TLS v1.1 (client only), but rejects older versions of the protocol. It supports the use of secp256r1, secp384r1, and secp521r1 elliptic curves during an ECDHE key exchange. The curve used depends upon the certificate supported and the peer's capabilities.

TLS client cipher suites using TLSv1.1 and TLSv1.2 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

TLS server cipher suites using TLSv1.2 are as follows:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

Verify the Revocation Status of a Certificate using OCSP

The device always performs an OCSP revocation-check on the certificate when the `authorityInfoAccess` extension is present and indicates that the `accessMethod` to use 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' the certificate is accepted.

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

NETCONF Log Support

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

```
device# copy support scp host <remote-host-ip-address> directory <dir> user <usr> 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 Log Support

The REST queries issued log information about the timestamp, URI, payload, METHOD, HTTP version, host IP, user, and 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> use-vrf <vrf-name>
```

All 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:

```
/var/log/restlog
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
```

Configure SSH Session Rekeying Intervals

SSH servers can trigger rekeying once a certain time interval is reached or data traffic reaches a specified volume. The SSH Server will rekey once the either of these thresholds is reached, resetting both thresholds. During rekeying, key exchange messages are transferred between the SSH client and the server, changing the session security key.

Rekeying by volume

Use the **rekey-volume** to configure the range of the rekey volume. The range is 512 to 1024 MB. The **rekey-volume** option cannot exceed a value equal to 1024 MB. The default value is 1024 MB.

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

Rekeying by time

Use the **rekey-interval** to configure the interval in seconds. The default value is 3600 seconds.

```
device(config)# 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 sent to a syslog server if configured. The device maintains two local logs: auditlog and raslog. The entries related to starting and terminating connections and the configuration commands issued are logged in the auditlog while the rest are in raslog. The auditlog and raslog can contain up to 1024 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 is recorded by a security-related event.

Access Method is how the event was triggered, and the access used for this event. The 5-tuple includes the username, privilege, and how the device is 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
```

Use the following command to display the latest logs and specify the number of entries:

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

A list of relevant audit log entries is in Appendix A: Audit Log Entries on page 33.

.

Appendix A: Audit Log Entries

REST and TLS Audit Log Entries

TABLE 2 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..
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.
Initiate RADIUS	18 AUDIT, 2020/08/27-16:40:30 (GMT), [SEC-3020], INFO, SECURITY, radiusadmin/admin/10.20.160.153/ssh/CLI,, SLX9540, Event: login, Status: success, Info: Successful login attempt via REMOTE, IP Addr: 10.20.160.153. 17 AUDIT, 2020/08/27-16:40:29 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/10.20.160.153/None/CLI,, A2, Event: TLS SESSION, TLS handshake, Info: Connecting to server: 10.20.160.153:5555. 16 AUDIT, 2020/08/27-16:40:29 (GMT), [SEC-3111], INFO, SECURITY, NONE/root/10.20.160.153/None/CLI,, A2, Event: TLS SESSION, TLS handshake, Info: Connecting to server: 10.20.160.153:5555.
Terminate RADIUS	19 AUDIT, 2020/08/27-16:40:30 (GMT), [SEC-3022], INFO, SECURITY, radiusadmin/admin/10.20.160.153/ssh/CLI,, SLX9540, Event: logout, Status: success, Info: Successful logout by user [radiusadmin].
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.

TABLE 2 REST and TLS-related Audit Log Entries (continued)

Operation	Log details
	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.
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.
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,

TABLE 2 REST and TLS-related Audit Log Entries (continued)

Operation	Log details
	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 Audit Log Entries

TABLE 3 OCSP and Certificate Audit Log Entries

Operation	Log Details
Certificate contains OCSP URI, but device encountered error in parsing	2020/08/09-17:40:52 (GMT), [SEC-3112], INFO, SECURITY, admin/admin/10.24.65.183/telnet/cli,, SLX, Event: X509v3, Certificate Validation failed, Info: Reason = failed to parse OCSP responder url,Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
OCSP Responder is not reachable	2020/08/09-17:18:50 (GMT), [SEC-3112], INFO, SECURITY, admin/admin/10.24.65.183/telnet/cli,, SLX, Event: X509v3, Certificate Validation failed, Info: Reason = OCSP application verification failure,Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
Certificate status is unknown	2020/08/09-16:17:40 (GMT), [SEC-3112], INFO, SECURITY, admin/admin/10.24.65.183/telnet/cli,, SLX, Event: X509v3, Certificate Validation failed, Info: Reason = certificate is unknown for OCSP,Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
Certificate status if revoked	2020/09/27-09:07:39 (GMT), [SEC-3112], INFO, SECURITY, admin/admin/127.0.0.1/console/cli,, SLX, Event: X509v3, Certificate Validation failed, Info: Reason = certificate is revoked to OCSP, Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
OCSP responder is reachable but returns failure.	2018/09/26-00:01:43 (GMT), [SEC-3112], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info: OCSP responder reports fail.Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.	14 AUDIT, 2020/08/09-17:21:14 (GMT), [SEC-3112], INFO, SECURITY, admin/admin/10.24.65.183/telnet/cli,, SLX, Event: X509v3,

TABLE 3 OCSP and Certificate Audit Log Entries (continued)

Operation	Log Details
	Certificate Validation failed, Info: Reason = unable to get issuer certificate,Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
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-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unable to decrypt certificate's signature. ,Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
The public key in the certificate SubjectPublicKeyInfo could not be read.	2018/09/26-00:01:43 (GMT), [SEC-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unable to decode issuer public key. Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
The signature of the certificate is invalid.	2018/09/26-00:01:43 (GMT), [SEC-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:certificate signature failure. Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
The certificate is not yet valid: the notBefore date is after the current time.	2018/09/26-00:01:43 (GMT), [SEC-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,,sw0, Event: X509v3, Certificate Validation failed, Info: Reaason = certificate is not yet valid. Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
The certificate has expired: that is the notAfter date is before the current time.	2021/09/27-09:05:52 (GMT), [SEC-3112], INFO, SECURITY, admin/ admin/127.0.0.1/console/cli,, SLX, Event: X509v3, Certificate Validation failed, Info: Reason = certificate has expired, Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
The certificate notBefore field contains an invalid time.	2018/09/26-00:01:43 (GMT), [SEC-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validationfailed, Info:format error in certificate's notBefore field Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
The certificate notAfter field contains an invalid time.	2018/09/26-00:01:43 (GMT), [SEC-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:format error in certificate's notAfter field Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
The passed certificate is self signed, and the same certificate cannot be found in the list of trusted certificates.	2020/08/09-17:28:33 (GMT), [SEC-3112], INFO, SECURITY, admin/ admin/10.24.65.183/telnet/cli,, SLX, Event: X509v3, Certificate Import, Info: Reason = self signed certificate, Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
The certificate chain could be built up using the untrusted certificates, but the root could not be found locally.	2021/09/27-08:59:11 (GMT), [SEC-3112], INFO, SECURITY, admin/ admin/127.0.0.1/console/cli,, SLX, Event: X509v3, Certificate Validation failed, Info: Reason = self signed certificate in certificate chain,Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
The issuer certificate of a locally looked up certificate could not be found. This normally means the list of trusted certificates is not complete.	2020/08/09-17:23:36 (GMT), [SEC-3112], INFO, SECURITY, admin/ admin/10.24.65.183/telnet/cli,, SLX, Event: X509v3, Certificate Validation failed, Info: Reason = unable to get local issuer certificate, Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <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-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unable to verify the first certificate Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
The certificate chain length is greater than the supplied maximum depth.	2018/09/26-00:01:43 (GMT), [SEC-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:certificate chain too long Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]

TABLE 3 OCSP and Certificate Audit Log Entries (continued)

Operation	Log Details
For the below scenario's we will get the audit logs: 1. A CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose. 2. When the basicConstraints field is not available in root ca	2020/08/31-14:07:56 (GMT), [SEC-3112], INFO, SECURITY, admin/ admin/134.141.219.247/telnet/ cli,, A2, Event: X509v3, Certificate Validation failed, Info: Reason = invalid CA certificate, Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
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-3112], INFO,SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, CertificateValidation failed, Info:invalid non-CA certificate (has CA markings). Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
The basicConstraints path-length parameter has been exceeded.	2018/09/26-00:01:43 (GMT), [SEC-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:path length constraint exceeded Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
The supplied certificate cannot be used for the specified purpose.	2020/08/09-16:27:18 (GMT), [SEC-3112], INFO, SECURITY, admin/ admin/10.24.65.183/telnet/cli,, SLX, Event: X509v3, Certificate Validation failed, Info: Reason = unsupported certificate purpose,Certificate Details = [Subject CN <CN>, Serial <serial no> Issuer <issuer>]
The root CA is not marked as trusted for the specified purpose.	2018/09/26-00:01:43 (GMT), [SEC-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:certificate not trusted. Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
The root CA is marked to reject the specified purpose.	2018/09/26-00:01:43 (GMT), [SEC-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:certificate rejected. Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
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-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:key usage does not include certificate signing Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
The certificate was rejected because its keyUsage extension does not include a digital signature.	2018/09/26-00:01:43 (GMT), [SEC-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:key usage does not include digital signature Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
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-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unsupported name constraint type. Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
The format of the name constraint is not recognized, 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-3112], INFO, SECURITY, NONE/ root/NONE/None/CLI,, sw0, Event: X509v3, Certificate Validation failed, Info:unsupported or invalid name constraint syntax. Certificate Details = [Subject CN <CN>,Serial <serial no> Issuer <issuer>]
Trust Anchor Add/remove Audits logs	266 AUDIT, 2020/10/20-01: 15:52 (GMT), [SEC-3091] , INFO, SECURITY, admin/admin/127.0.0.1/console/cli,, SLX9640, Event: Crypto Ca Trustpoint, Status: success, Info: Crypto CA Trustpoint is created. 265 AUDIT, 2020/10/20-01: 15:29 (GMT), [SEC-3099] , INFO, SECURITY, admin/admin/127.0.0.1/console/cli,, SLX9640, Event: Crypto Ca https, Status: success, Info: Crypto CA Trustpoint is Deleted.
The basicConstraints parameter is false for CA certificate.	29 AUDIT, 2020/10/16-20:24:26 (GMT), [SEC-3112], INFO, SECURITY, admin/admin/127nvalid CA certificate: basic constraints false for CA, Certificate Details = [Subject CN Rootca, Serial 606515782677152643827449854615400486099997772896 Issuer /C=IN/ST=KA/L=Ban

TABLE 3 OCSP and Certificate Audit Log Entries (continued)

Operation	Log Details
CN/SAN mismatch	54 AUDIT, 2020/10/16-21:09:23 (GMT), [SEC-3112], INFO, SECURITY, admin/admin/127.0.0.1/console/cli,, SLX, Event: X509v3, Certificate Validation failed, Info: Reason = Common name does not match host IP Certificate Details = [Subject CN 10.20.238.152, Serial 4096 Issuer /C=IN/ST=KA/O=Extreme/OU=engg/CN=Intermediateca].

SSH Audit Log Entries

TABLE 4 SSH Audit Log Entries

Operation	Log Details
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 todiffie-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	2020/10/07-08:14:51, [SEC-3113], 57,, INFO, SLX9150-48Y, Event: SSH SESSION, SSH PROTOCOL, Info: Peer 10.20.160.154 sent an unsupported host key 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	2020/10/07-08:14:51, [SEC-3113], 57,, INFO, SLX9150-48Y, Event: SSH SESSION, SSH PROTOCOL, Info: Peer 10.20.160.154 sent an unsupported hash algorithm list
Unsupported key exchange algorithm	65 AUDIT, 2020/10/07-10:12:41 (GMT), [SEC-3113], INFO, SECURITY, admin/admin/134.141.219.157/telnet/cli,, SLX9150-48Y, Event: SSH SESSION, SSH PROTOCOL, Info: Peer 10.20.238.152 sent an unsupported key exchange algorithm list
Key exchange algorithm does not match	49 AUDIT, 2020/10/07-08:31:02 (GMT), [SEC-3113], INFO, SECURITY, admin/admin/127.0.0.1/console/cli,, SLX9150-48Y, Event: SSH SESSION, SSH PROTOCOL, Info: Peer 10.24.65.107 sent an unsupported encryption algorithm list.
Rekey interval expired	69 AUDIT, 2020/08/28-09:24:24 (GMT), [SEC-3113], INFO, SECURITY, admin/admin/127.0.0.1/ssh/cli,, SLX9250-32C, Event:

TABLE 4 SSH Audit Log Entries (continued)

Operation	Log Details
	SSH SESSION, SSH PROTOCOL, Info: Rekeying session of user admin as rekey interval expired.
Rekey Volume has reached	64 AUDIT, 2020/08/28-20:21:11 (GMT), [SEC-3113], INFO, SECURITY, admin/root/127.0.0.1/ssh/cli,, SLX9250-32C, Event: SSH SESSION, SSH PROTOCOL, Info: Rekeying session of user root as rekey volume has reached
Oversized packet error	80 AUDIT, 2020/10/07-10:19:04 (GMT), [SEC-3023], INFO, SECURITY, NONE/root/NONE/None/CLI,, sw0, Event: SSH SESSION, Packet Size Error, Info: Peer 10.20.238.152 sent a packet of invalid length 270056785.
Unsupported encryption algorithm	48 AUDIT, 2020/10/07-08:27:06 (GMT), [SEC-3113], INFO, SECURITY, admin/admin/127.0.0.1/console/cli,, SLX9150-48Y, Event: SSH SESSION, SSH PROTOCOL, Info: Peer 10.24.65.107 sent an unsupported encryption algorithm list.
Encryption algorithm does not match	65 AUDIT, 2020/10/07-10:12:41 (GMT), [SEC-3113], INFO, SECURITY, admin/admin/134.141.219.157/telnet/cli,, SLX9150-48Y, Event: SSH SESSION, SSH PROTOCOL, Info: Peer 10.20.238.152 sent an unsupported key exchange algorithm list
Unsupported MAC integrity algorithm	43 AUDIT, 2020/10/07-08:21:27 (GMT), [SEC-3113], INFO, SECURITY, admin/admin/127.0.0.1/console/cli,, SLX9150-48Y, Event: SSH SESSION, SSH PROTOCOL, Info: Peer 10.24.65.107 sent an unsupported mac list
User is locked out once certain number of retries with invalid credentials is reached	80 AUDIT, 2020/10/07-10:19:04 (GMT), [SEC-3023], INFO, SECURITY, user/NONE/NONE/None/CLI,, SLX, Event: login, Status: failed, Info: Account [user] locked, failed password attempts exceeded.

NTP Log Entries

TABLE 5 NTP Log Entries

Operation	Log Details
Add an NTP server	68 AUDIT, 2020/08/28-20:23:24 (GMT), [DCM-1006], INFO, DCMCFG, admin/admin/127.0.0.1/console/cli,, SLX, Event: database commit transaction, Status: Succeeded, User command: "configure config ntp server 10.20.232.221".
Remove an NTP server	70 AUDIT, 2020/08/28-09:27:05 (GMT), [DCM-1006], INFO, DCMCFG, admin/admin/127.0.0.1/console/cli,, SLX, Event: database commit transaction, Status: Succeeded, User command: "configure config no ntp server 10.20.232.221".
NTP client association is started	2020/03/24-11:50:51, [TS-1020], 154,, INFO, SLX, client association is mobilized for 10.24.12.107
NTP Stratum is changed	2020/03/24-11:52:34, [TS-1018], 157,, INFO, SLX, Stratum is changed to 3
NTP clock is synchronized	2020/03/24-11:52:35, [TS-1019], 158,, INFO, SLX, System clock is synchronized to 10.24.12.107 previous time was Tue Mar 24 11:52:34 2020

Miscellaneous Entries

Operation	Log Details
Startup: BOMAudit message log is enabled	5 AUDIT, 2020/08/28-18:11:37 (GMT), [RAS-2001], INFO, RAS, NONE/root/NONE/None/CLI,, SLX, Audit message log is enabled.
Shutdown: BOMSystem is about to reload. No auditlog observed as "System is about to reload.	0 AUDIT, 2020/08/28-18: 10:55 (GMT), [HASM-1004], INFO, SECURITY, NONE/root/NONE/None/CLI,, SLX9250-32C, SW/0 BOMSystem is about to reload.
User is locked out once certain number of retries with invalid credentials is reached	80 AUDIT, 2020/10/07-10:19:04 (GMT), [SEC-3023], INFO, SECURITY, user/NONE/NONE/None/CLI,, SLX, Event: login, Status: failed, Info: Account [user] locked, failed password attempts exceeded.
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 and Download Audit Log Entries

TABLE 6 Firmware Update and Download Audit Log Entries

Operation	Log Details
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

TABLE 7 Console Login Audit Log Entries

Operation	Log details
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

TABLE 7 Console Login Audit Log Entries (continued)

Operation	Log details
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 Message 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 algo algorithm(SHA1)...successful. b. Included
algorithm (D-H)...successful

2. Automatic power-up self test: a. FIPS RNG (AES_256_CTR_DRBG) selftest...successful

3. AES-128CBC encryption/decryption...successful

4. RSA key generation andencryption/decryption...successful (4.1) RSA 2048 with 'SHA256'
testing...successful

5. TDES-CBC encryption/decryption...successful

6a) SHA-1hash...successful 6b) SHA-256 hash...successful 6c) SHA-384 hash...successful 6d) SHA-512
hash...successful 6e) HMAC-SHA-1hash...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 (SHA1)...Notexecuted b)Included
algorithm (D-H)...successful as expected

8. Zero-ization...Successful

9. TLS KDF 1.0...successful  a)TLS KDF1.2...successful

10. ECDSA ...successful

11. ECDH...successful

All tests completed with 0 errors
```

Wheneach test observes failure, 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 ...
```

Appendix B: X.509v3 SSH Authentication

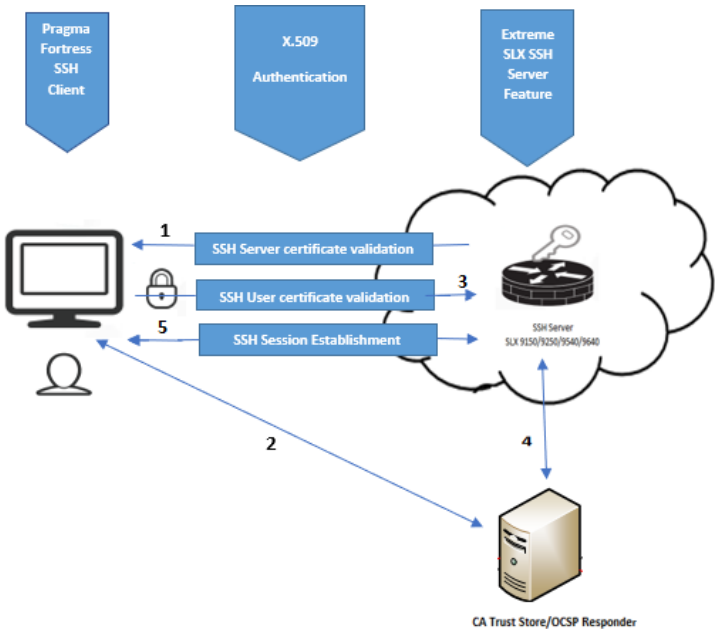
Overview of X.509v3 Authentication

This appendix documents how to configure a secure shell (SSH) authentication using an X.509v3 digital certificate.

Third-party software used: Pragma Fortress/SecureCRT SSH client

Linux tools used: OpenSSL

FIGURE 1 Flow diagram of SSH X.509 authentication



X.509v3 SSH Server Configuration

On the SLX-OS device, configure an SSH server using an X.509v3 certificate.

1. Configure key-pair and trustpoint.

```
device# configure terminal
device(config)# crypto key label <key name> <key type> modulus <key size>
device(config)# crypto ca trustpoint <trustpoint name>
device(config-ca-<>)# keypair <key name>
device(config-ca-<>)# end
```

2. Import root CA certificate used to sign SSH server certificate, as described in Generate Root CA and Sign Host Certificate on page 45.

```
device# [no] crypto ca authenticate <trustpoint> cert-type [sshx509v3] protocol <> directory <> file
<> host <> user <> password <>
```

3. Sign CSR and send it to the external Linux server.

NOTE
Use management IP or inband interface IP as common.

```
device# crypto ca [enroll] <trustpoint> cert-type [sshx509v3] country <> state <> locality <>
organization <> orgunit <> common <> protocol <> directory <> host <> user <> password <>
```

4. Sign end-entity certificate from the CSR using the Linux server OpenSSL tool.

```
# openssl ca -policy policy_loose -extensions server_cert -out <cert file name> -config openssl.cnf -
infiles <cert signing request>
```

NOTE
For example, see Sample openssl.cnf on page 47,

5. Import end-entity server certificate to the device.

```
device# [no] crypto ca [import] <trustpoint> cert-type [sshx509v3] protocol <> directory <> file <>
host <> user <> password <>
```

6. Configure algorithm accepted by the SSH server for server authentication. Only the configured algorithm negotiates with the secure shell (SSH) client.

```
device(config)# [no] ssh server algorithm hostkey <x509v3-ssh-rsa | x509v3rsa2048-sha256>
```

7. For server authentication, the SSH server sends its certificate to the SSH client for validation. Associate this servercertificate with SSH through SSH server certificate profile trustpoint configuration.

```
device(config)# [no] ssh server certificate profile server
device(ssh-server-cert-profile-server)# trustpoint sign <trustpoint name>
```

8. After configuring the SSH server algorithm and trustpoint, restart the SSH server.

```
 device#ssh-server restart
```

X. x509-v3 SSH User Configuration

Configure an SLX-OS user for SSH X.509 certificate validation and authentication.

1. Configure the new user or use the default user.

```
device(config)# username <> role <> password <>
```

2. Import the root CA used to sign user certificate, as described in Generate Root CA and Sign Host Certificate on page 45.

```
device# [no] crypto import sshx509v3ca protocol <> host <> directory <> file <> user <> password <>
```

3. Configure SSH user certificate Distinguished Name (DN) to SSH server.

NOTE
Distinguished Name (DN) is the subject taken from the user certificate. Refer to step 15 of Generate Root CA and Sign Host Certificate on page 45.

```
device# [no] certutil sshx509v3 user <> DN <>
```

4. After the certificate import and DN configuration, restart the SSH server.

```
device#ssh-server restart
```

5. Configure Pragma Fortress SSH client, as described at https://www.pragmasys.com/ssh-client/index.htm?context=550.

Generate Root CA and Sign Host Certificate

In OpenSSL, generate the root Certificate Authority (CA) and sign the host certificate using a set of commands. These commands are not available on the SLX platform and require the administrator to set up a Linux platform and install OpenSSL. If the organization intends to use certificates from a valid authority such as Verisign, follow the provider's instructions from the certificates obtained.

The task provided in this section is an example of a "self" signed implementation of a certificate authority (CA) and subsequent host certificates.

1. Enter the following commands.

```
# mkdir /root/<dir>
# cd /root/<dir>
# mkdir certs crl newcerts private
# chmod 700 private
# touch index.txt
# echo 1000 > serial
```

2. Prepare the configuration file, as described in Sample openssl.cnf on page 47, changing "dir" to "/root/<dir>".

```
# cp openssl.cnf
```

3. Create the root key.

```
# cd root/<dir>
#openssl genrsa -aes256 -out private/ca.key.pem 4096
#chmod 400 private/ca.key.pem
```

4. Create the root certificate.

```
# cd root/<dir>
# openssl req -config openssl.cnf -key private/ca.key.pem -new -x509 -days 7300 -sha256 -extensions
v3_ca -out certs/ca.cert.pem
Country Name (2 letter code) [GB]:IN
State or Province Name [England]:KA
Locality Name []:Bangalore
Organization Name [Alice Ltd]:Extreme
Organizational Unit Name []:Engg
Common Name []:EMIS Root CA
Email Address []:
# chmod 444 certs/ca.cert.pem
```

5. Verify the root certificate.

```
# openssl x509 -noout -text -in certs/ca.cert.pem
```

6. Sign the OCSP responder CSR request.

```
# openssl req -config openssl.cnf -new -sha256 -key private/ca.key.pem -out certs/
userx509v3_ocsp.csr.pem
```

7. Enter pass phrase for `private/ca.key.pem`.

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-------
Country Name (2 letter code) [GB]:IN
State or Province Name [England]:KA
Locality Name []:Bangalore
Organization Name [Alice Ltd]:Extreme
Organizational Unit Name []:EMIS User OCSP
Common Name []:10.24.12.107
Email Address []:
```

8. Sign the OCSP Responder end-entity certificate using the CSR.

```
# openssl ca -config openssl.cnf -extensions ocsp -days 375 -notext -md sha256 -in certs/
userx509v3_ocsp.csr.pem -out certs/userx509v3_ocsp.cert.pem
# chmod 444 certs/userx509v3_ocsp.cert.pem
```

9. Verify the OCSP responder certificate chain.

```
# openssl verify -CAfile certs/ca.cert.pem certs/userx509v3_ocsp.cert.pem
certs/userx509v3_ocsp.cert.pem: OK
```

10. Sign User certificate signing request.

```
# openssl req -config openssl.cnf -key private/ca.key.pem -new -sha256 -out certs/
testuser_test1.csr.pem
Enter pass phrase for private/ca.key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-------
Country Name (2 letter code) [GB]:IN
State or Province Name [England]:KA
Locality Name []:Bangalore
Organization Name [Alice Ltd]:Extreme
Organizational Unit Name []:EMIS User
Common Name []:testuser
Email Address []:[
```

11. Sign User end-entity certificate using the CSR.

NOTE

Use extension “usr_cert” as it is used for user authentication.

```
# openssl ca -config openssl.cnf -policy policy_loose -extensions usr_cert days 375 -notext -md
sha256 -in certs/testuser_test1.csr.pem -out certs/testuser_test1.cert.pem
# chmod 444 certs/testuser_test1.cert.pem
```

12. Verify the user certificate chain.

```
# openssl verify -CAfile certs/ca.cert.pem certs/testuser_test1.cert.pem
certs/testuser_test1.cert.pem: OK
```

13. Run OCSP responder on TCP port 2568 for clients from the device to send OCSP requests.

```
# openssl ocsp -port 2568 -text -sha256 -index index.txt -CA certs/ca.cert.pem -rkey private/
ca.key.pem -rsigner certs/testuser_ocsp.cert.pem -nrequest 5
```

14. Convert the .pem certificate to a .pfx certificate.

```
# openssl pkcs12 -export -out testuser_test1.pfx -inkey ../private/ca.key.pem -in
testuser_test1.cert.pem -certfile ca.cert.pem
```

15. Get the subject DN details of a certificate.

```
# openssl x509 -noout -text -subject -in testuser_test1.cert.pem
```

Sample openssl.cnf

This is a sample OpenSSL configuration file.

```
# cat openssl.cnf
# OpenSSL root CA configuration file.
# Copy to your working directory root/<dir>/openssl.cnf`.

[ ca ]
# `man ca`
default_ca = CA_default

[ CA_default ]
# Directory and file locations.
dir               = /root/<dir>
```

```
certs             = $dir/certs
crl_dir           = $dir/crl
new_certs_dir     = $dir/newcerts
database          = $dir/index.txt
serial            = $dir/serial
RANDFILE          = $dir/private/.rand

# The root key and root certificate.
private_key       = $dir/private/ca.key.pem
certificate       = $dir/certs/ca.cert.pem

# For certificate revocation lists.
crlnumber         = $dir/crlnumber
crl               = $dir/crl/ca.crl.pem
crl_extensions    = crl_ext
default_crl_days = 30

# SHA-1 is deprecated, so use SHA-2 instead.
default_md        = sha256

name_opt          = ca_default
cert_opt          = ca_default
default_days      = 375
preserve          = no
policy            = policy_strict

[ policy_strict ]
# The root CA should only sign intermediate certificates that match.
# See the POLICY FORMAT section of `man ca`.
countryName             = match
stateOrProvinceName     = match
organizationName        = match
organizationalUnitName = optional
commonName              = supplied
emailAddress            = optional

[ policy_loose ]
# Allow the intermediate CA to sign a more diverse range of certificates.
# See the POLICY FORMAT section of the `ca` man page.
countryName             = optional
stateOrProvinceName   =   optional
localityName            = optional
organizationName     =     optional
organizationalUnitName  =  optional
commonName              = supplied
emailAddress            = optional

[ req ]
# Options for the `req` tool (`man req`).
default_bits        = 2048
distinguished_name = req_distinguished_name
string_mask         = utf8only

# SHA-1 is deprecated, so use SHA-2 instead.
default_md          = sha256

# Extension to add when the -x509 option is used.
x509_extensions     = v3_ca

[ req_distinguished_name ]
# See <https://en.wikipedia.org/wiki/Certificate_signing_request>.
countryName                     = Country Name (2 letter code)
stateOrProvinceName             = State or Province Name
localityName                    = Locality Name
0.organizationName              = Organization Name
organizationalUnitName          = Organizational Unit Name
commonName                      = Common Name
emailAddress                    = Email Address

# Optionally, specify some defaults.
countryName_default             = IN
stateOrProvinceName_default = KA
```

```
localityName_default            =
0.organizationName_default      = Extreme
organizationalUnitName_default =
emailAddress_default            =

[ v3_ca ]
# Extensions for a typical CA (`man x509v3_config`).
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ v3_intermediate_ca ]
# Extensions for a typical intermediate CA (`man x509v3_config`).
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ usr_cert ]
# Extensions for client certificates (`man x509v3_config`).
basicConstraints = CA:FALSE
nsCertType = client, email
nsComment = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, emailProtection
authorityInfoAccess = OCSP;URI:http://x.x.x.x.:2568

[ server_cert ]
# Extensions for server certificates (`man x509v3_config`).
basicConstraints = CA:FALSE
nsCertType = server
nsComment = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
authorityInfoAccess = OCSP;URI:http://x.x.x.x:2567

[ crl_ext ]
# Extension for CRLs (`man x509v3_config`).
authorityKeyIdentifier=keyid:always

[ ocsp ]
# Extension for OCSP signing certificates (`man ocsp`).
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, digitalSignature
extendedKeyUsage = critical, OCSPSigning
[root@rhel-105-201 user]#
```

Appendix C: NTP

Network Time Protocol Overview

Network Time Protocol (NTP) maintains uniform time across all devices in a network. The NTP commands support an external time server's configuration to maintain synchronization among all local clocks in a network.

To keep the time in your network current, it is recommended that each device have its time synchronized with at least one external NTP server.

Date and Time Settings

Extreme devices maintain the current date and time inside a battery-backed real-time clock (RTC) circuit. Date and time are used for logging events. Device operation does not depend on the date and time; a device with incorrect date and time settings can function correctly. However, because the date and time are used for logging, error detection, and troubleshooting, you should set them correctly.

Time Zone Settings

The time zone settings have the following characteristics:

- Adjusts for Daylight Savings Time automatically.
- Changes the time zone on a device updates the local time zone setup and is reflected in local time calculations.
- By default, all devices are in the Greenwich Mean Time (GMT) time zone (0,0).
- System services that are started will reflect the time zone changes only after the next reboot.
- Persist across failover for high availability.
- Are not affected by NTP server synchronization.

Network Time Protocol Server Overview

The NTP server provides the correct network time on your device and synchronizes the time on devices across a network. It obtains the correct time from an external time source and adjusts the local time in each connected device. When the NTP server functionality is enabled, the NTP server starts listening to the NTP port for client requests and responds with the reference time. The NTP server is stateless and does not maintain NTP client information. Network time synchronization is guaranteed when all devices use a common external time server.

Configure up to eight server addresses in IPv4 or IPv6 format. When configuring multiple NTP server addresses, the NTP algorithm finds the most reliable server and uses this as the active NTP server. If there are no reachable time servers, then the local device time becomes the default time until a new configured active time server. If an NTP server loses synchronization, it operates in master mode to serve time using the local clock. Use the ntp master command to enable the serving of local time.

IMPORTANT
Although time-stepping corrects a large offset after a reload, as a best practice, do not manually change the time after NTP synchronization.

Network Time Protocol Client Overview

When configuring one or more NTP servers/peers, you can enable a NTP client. The NTP client maintains the server and peer state information as an association. The server and peer association is mobilized at startup or after it has been configured. A statically configured server/peer association is not demobilized unless the configuration is removed/changed. A symmetric passive association is mobilized upon an NTP packet's arrival from a not statically configured peer. This type of association is demobilized on error or timeout. The NTP client operation can be summarized as follows:

1. The device is booted, and the system initializes. The configured servers and peers are polled at the configured poll interval. Additional dynamically discovered servers/peers are also polled.
2. Multiple samples of server/peer times in the NTP packet are added to and maintained in the association database.
3. The selection, cluster and combine algorithms choose the most accurate and reliable server/peer as system peer.

   NOTE
   Refer to RFC5905.

4. The reference time from the system peer is used for system time synchronization.
5. The NTP client increases the poll interval from the minimum poll interval to the maximum poll interval value after the clock stabilizes.

After choosing the system peer, the system time is synchronized using one of the following ways:

- If the system time differs from the system peer by less than 128 milliseconds, the system clock is adjusted slowly towards the system peer time reference time.
- If the system time differs from the system peer by greater than 128 milliseconds, the system clock is stepped to the system peer reference time. The old, time-related information stored in the server/peer association database is cleared.

Network Time Protocol Associations

NTP works in one or more association modes. The following modes are the NTP polling-based associations:

- NTP Server
- NTP Client

- NTP Peer

NTP Server

The Server mode requires no prior client configuration; it responds to Client mode NTP packets. Use the `ntp server enable` command to set the device to operate in Server mode. Use `no ntp disable serve` to ensure NTP is configured in server mode. SLX allows for eight NTP servers to be configured and allows the version to be selectable between NTP version 3 and 4.

NTP Client

When the system is operating in Client mode, all configured NTP servers and peers are polled. The device selects a host from all the polled NTP Servers from which to synchronize. To configure the NTP servers and peers individually, use the `server` and `peer` commands.

NTP Peer

NTP Peer mode is intended for configurations where a group of devices operates as a mutual backup for one another. If one device loses a reference source, the time values flow from the remaining peers. The NTP peer can operate in:

- **Symmetric Active** - When the peer is configured using the peer command.
- **Symmetric Passive** - If the device is not configured using the peer command, an NTP packet's arrival from a symmetric active peer generates a symmetric passive response. However, to prevent introducing false time values, authentication in symmetric mode is strongly suggested.

Network Time Protocol Authentication

NOTE
NTP Authentication MUST only use SHA1 to maintain a Common Criteria validated configuration.

Configure NTP to provide cryptographic authentication of messages with the clients/peers and upstream time server. NTP supports symmetric key scheme for authentication. The scheme must only use SHA1 authentication algorithms: the key-id and the calculated digest form the Message Authentication Code (MAC). When enabling authentication on the server, it is expected that the client's request message has a valid MAC. If authentication of the client message fails, NTP replies with a crypto-NAK packet.

Enable NTP Authentication

```
device(config)# ntp authenticate
Syntax: [no] ntp authenticate
```

1. To enable NTP strict authentication, use the `authenticate` command.
2. To disable the function, use the `no` form of this command.

Defining an Authentication Key

```
device(config)# ntp authentication-key 10 sha1 teststring encryption-level 0
Full Syntax: [no] ntp authentication-key <key-id> <Auth-Type sha1>
<Auth-String> encryption-level <0/7>
```

1. To enable NTP strict authentication, use the `authenticate` command.

The valid key-id parameter is 1 to 65535. The key type MUST be SHA1 to maintain a Common Criteria validated configuration. SHA1 specifies message authentication support provided using the SHA1 algorithm. Auth String; secret key string. Encryption level 0/7; 0 is clear text, 7 is encrypted text.

2. To disable the function, use the `no` form of this command.

NTP Trusted Keys

Trusted keys are keys within the set of configured keys used to synchronize a device to a trusted server and prevent synchronization with a non-trusted device. While it is possible to synchronize a server to a client with only an Authentication key, synchronizing a client to a server requires that an NTP Authentication be enabled on both the client and server. The same trusted keys are specified on each device. The keys configured for server/peer are implicitly considered trusted keys.

NOTE

Configure the key as an authentication-key before you add it as a trusted key.

```
device(config)# [no] ntp trusted-key 10 20
Full syntax: [no] ntp trusted-key <key-id-list>
```

1. To define an NTP Trusted Key, use the `ntp trusted-key` command.

   Key-id: The allowed range is 1-65535. Use the `ntp authentication-key` command to configure a maximum of 10 trusted keys.

2. To remove an NTP Trusted Key, use the `no` form of this command.

Configuring NTP

After setting the date and time on a device, synchronize the local time on a device with a NTP server.

Set the date and time in privileged EXEC mode and only has to be configured once per device. The value is written to nonvolatile memory. After setting the basic time information, configure an NTP server to synchronize the local time across the network.

1. Set the current date and time using the UTC time zone. Otherwise, issues arise as NTP attempts to sync to the upstream servers and peers, and the clock time zone command adjusts the time incorrectly.

   ```
   device# clock set 2016-08-06T12:15:00
   ```

2. Access global configuration mode.

   ```
   device# configure terminal
   ```

3. Set the time zone for the device.

   ```
   device(config)# clock timezone America/Los_Angeles
   ```

4. Return to privileged EXEC mode.

   ```
   device(config)# exit
   ```

5. Display the local date, time, and time zone for the device.

   ```
   device# show clock
   2017-02-09 12:15:00 America/Los_Angeles
   ```

6. Enter global configuration mode.

   ```
   device# configure terminal
   ```

7. Synchronize the local time with an external source accessible from a user-specified VRF named myvrf.

```
device(config)# ntp server 192.168.10.1 use-vrf myvrf
```

8. Exit to global configuration mode.

```
device(config)# exit
```

9. Exit to privileged EXEC mode.

```
device(config)# exit
```

10. Display the active NTP server IP address.

```
device# show ntp status
Clock is synchronized, stratum 3, reference clock is 192.168.128.5
precision is 2**24
reference time is CC38EC6A.8FCCA1C4 (10:10:02.561 JST Fri Jan 20 2017)
clock offset is -1.051 msec, root delay is 174.060 msec
root dispersion is 172.37 msec, peer dispersion is 0.10 msec
system poll interval is 32, last update was 19 sec ago
NTP server mode is enabled, NTP client mode is enabled
NTP master mode is disabled, NTP master stratum is 8
```

11. To add additional NTP servers, repeat this process.
12. In a Common Criteria configuration, NTP will require an access list to be configured and added to the ports active in the switch. The following commands need to be utilized to with some variable information.

Variable	Description
ACL_Name	A unique name to identify the Access Control List.
NTP Server IP	IP address assigned to NTP server authorized to communicate with the device.
Switch Management IP	IP Address assigned to the switch for management purposes.

```
device# ip access-list extended <ACL_NAME>
seq 10 permit udp host <NTP Server IP> host <Switch Management IP> eq ntp count log
            ** If more than one is allowed another instance of the above will be needed.
seq 20 deny udp any any eq ntp count log
seq 30 permit ip any any count log
```

In the following example, the date, time, and time zone are set on a device and verified. Configure the local device to synchronize the local time with an external NTP server at a specific IP address, accessible from a user-specified VRF named myvrf.

```
device# clock set 2017-02-09 12:15:00
device# configure terminal
device(config)# clock timezone America/Los_Angeles
device(config)# exit
device# show clock
2017-02-09 12:15:00 America/Los_Angeles
device# configure terminal
device(config)# ntp server 192.168.10.1 use-vrf myvrf
device(config)# exit
device(config)# exit
device# show ntp status
Clock is synchronized, stratum 3, reference clock is 192.168.128.5
precision is 2**24
reference time is CC38EC6A.8FCCA1C4 (10:10:02.561 JST Fri Jan 20 2017)
clock offset is -1.051 msec, root delay is 174.060 msec
root dispersion is 172.37 msec, peer dispersion is 0.10 msec
system poll interval is 32, last update was 19 sec ago
NTP server mode is enabled, NTP client mode is enabled
NTP master mode is disabled, NTP master stratum is 8
```

Authenticating an NTP server

Create an authentication key and associate the key to an NTP server.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Create an authentication key ID and key string.

```
device(config)# ntp authentication-key 33 sha1 check
```

Configure up to 10 NTP authentication keys, and each key ID must be unique.

3. Synchronize the local time with an external source, an NTP server, accessible by the management VRF. Associate the key to the NTP server.

```
device(config)# ntp server 192.168.10.1 key 33
```

4. Exit to global configuration mode

```
device(config)# exit
```

5. Exit to privileged EXEC mode.

```
device(config)# exit
```

6. To add additional NTP authentication keys, repeat this process. Configure up to 10 NTP authentication keys, and each key ID must be unique.

In the following example, an authentication key with an ID of 33 is created and the local time on the device is synchronized with an external NTP server at the IP address of 192.168.10.1.

```
device# configure terminal
device(config)# ntp authentication-key 33 sha1 check
device(config)# ntp server 192.168.10.1
device(config)# server-192.168.10.1 key 33
device(config)# exit
device(config)# exit
device(config)# ntp authenticate
```

Displaying the Active NTP Server

Displaying the Active NTP Server

A configured NTP server displays the server IP address. If not configured or the server is unreachable, LOCL (for the NTP server's local device time) displays.

NTP server status when an NTP server is not configured

The following example shows the status of a configured NTP server:

```
device# show ntp status
Clock is unsynchronized, no reference clock.
```

```
NTP server mode is enabled, NTP client mode is enabled
NTP master mode is disabled
```

NTP server status when an NTP server is configured

The following example shows the status of a configured NTP server:

```
device# show ntp status
Clock is synchronized, stratum 3, reference clock is 192.168.128.5
precision is 2**24
reference time is CC38EC6A.8FCCA1C4 (10:10:02.561 JST Fri Jan 20 2017)
clock offset is -1.051 msec, root delay is 174.060 msec
root dispersion is 172.37 msec, peer dispersion is 0.10 msec
system poll interval is 32, last update was 19 sec ago
NTP server mode is enabled, NTP client mode is enabled
NTP master mode is disabled, NTP master stratum is 8
```