ExtremeXOS Common Criteria Configuration Guide

31.3.100

9037401-00 Rev AA
November 2022

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, 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: https://www.extremenetworks.com/support/policies/open-source-declaration/

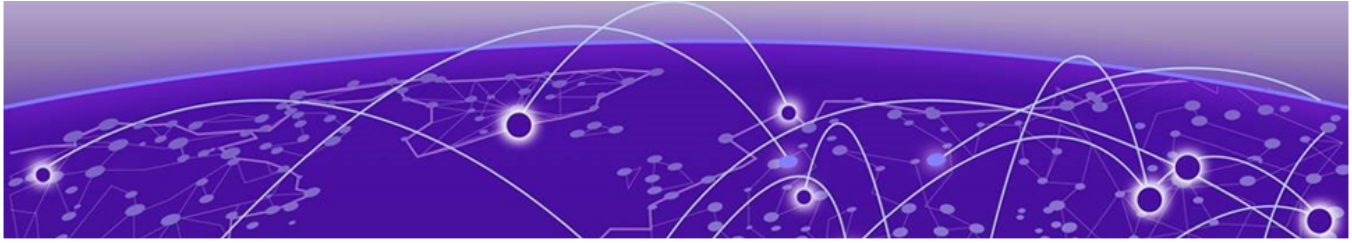


Table of Contents

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Conventions

To help you better understand the information presented in this guide, the following topics describe the formatting conventions used for notes, text, and other elements.

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.

Important
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.

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

Text formatting conventions

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

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

Command syntax conventions

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

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

Documentation and Training

Find Extreme Networks product information at the following locations:

- Current Product Documentation
- Release Notes
- Hardware and software compatibility for Extreme Networks products
- Extreme Optics Compatibility
- Other resources such as 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/.

Help and Support

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 Product Announcements

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

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

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

Send Feedback

The Information Development team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you

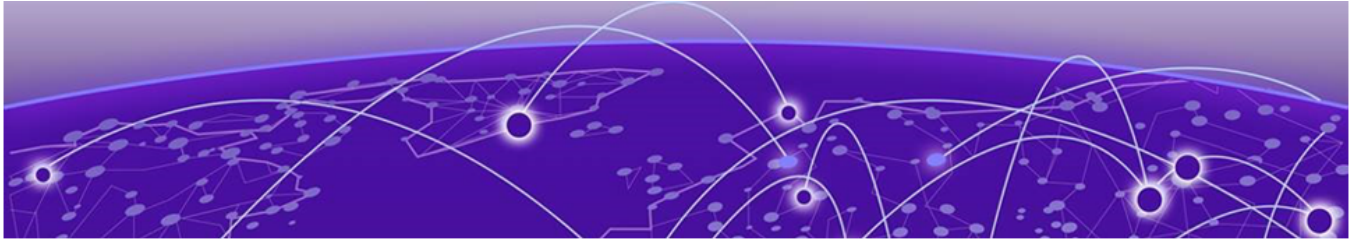
in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

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

To send feedback, do either of the following:

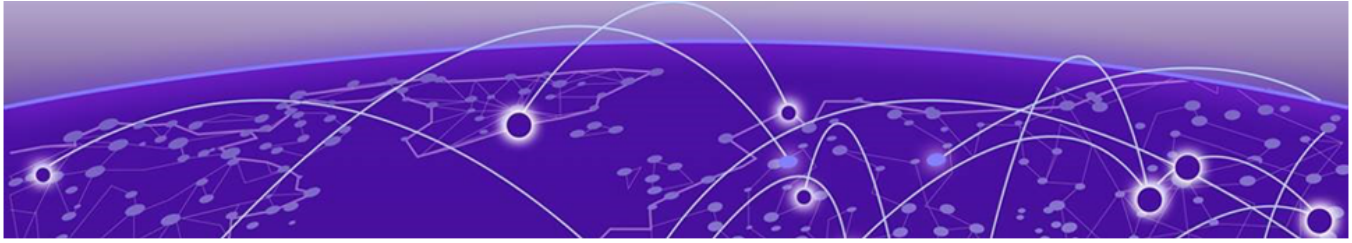
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

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

This document is new for the ExtremeXOS® 31.3.100 release.



Common Criteria Certification Configuration

Common Criteria certification for a device enforces a set of security standards, and limits features to comply with Common Criteria standards.

When administrators log in with role-based credentials, their access is limited to commands they have privileges and permissions to use based on Common Criteria standards. Also, network management communication paths are protected against modification and disclosure using SSHv2 and TLS. The audit channel to an external syslog server is protected using TLS encapsulation.

All security management functions are restricted to a valid administrator with the `admin` role.

FIPS 140-2 Security Level 1 specifies the security requirements that are satisfied by a cryptographic module used in a security system that protects a system's sensitive information.

Common Criteria compliance mode supports devices running EXOS version 31.3.100. Cryptographic Algorithm Validation Program (CAVP) certifies all cryptographic algorithms required by and used in Common Criteria.

Evaluated Configuration

The following switches, running EXOS version 31.3.100, were evaluated for compliance.

- X435
- X440-G2
- X460-G2
- X465
- X695-48Y-8C
- 5520

Establish a Serial Connection

Connect a terminal to the serial console interface to monitor and configure the system directly.

Before You Begin

To use the console port, you need the following equipment:

- A terminal or TeleTypewriter (TTY)-compatible terminal, or a portable computer with a serial port and terminal-emulation software.
- A specific cable with an RJ–45 or USB connector for the console port on the device. The other end of the cable must use a connector appropriate to the serial port on the computer or terminal.

To comply with emissions regulations and requirements, you must shield the cable that connects to the console port.

Procedure

1. Configure the terminal protocol as follows.

   9600 baud or 115200 baud, depending on the hardware platform
   8 data bits
   1 stop bit
   No parity
   No flow control
2. Connect the RJ-45 or USB cable to the console port on the device.
3. Connect the other end of the cable to the terminal or computer serial port.
4. Turn on the terminal.
5. Log on to the device.

Configure the Out-of-Band Management Interface

Configure the IP address for the management interface so you can remotely access the device using the out-of-band management port.

About This Task

Some models of the x435 device do not include an out-of-band management interface. To configure the management interface for those models, see Configure the In-Band Management Interface on page 12.

Procedure

1. Define the host name for the device.

```
# configure snmp sysname X468
```

   This example defines X468 as the host name.
2. Configure the IP address and mask for the management port.

```
# configure vlan Mgmt
ipaddress <ip-address> <netmask>
```

   In the command, you can specify the VLAN by its name or its ID. In this example, the VLAN name is "Mgmt."
3. Configure the IP routes for the management network.

```
# configure iproute add default <gateway> vr <vr-name>
```

4. Verify the management IP interface information.

```
# show mgmt
```

5. Save the configuration.

```
# save configuration
```

Configure the In-Band Management Interface

Configure the IP address for the management interface so you can remotely access the device using the in-band port with a management VLAN.

About This Task

The following models of the X435 device do not include an out-of-band management interface.

- X435-8T-4S
- X435-8P-4S
- X435-8P-2T-W

For these models, you can configure an in-band management interface on a management VLAN.

Procedure

1. Create a management virtual router.

```
# create virtual-router VR-Mgmt
```

   This example creates a virtual router named VR-Mgmt.
2. Create a management VLAN that is associated with the virtual router.

```
# create vlan Mgmt vr VR-Mgmt tag <802.1Q tag>
```

   This example creates a VLAN named "Mgmt" that is associated with a virtual router named "VR-Mgmt" and assigned an 8.2.1Q tag. Valid values for the tag range from 2 to 4095.
3. Configure the IP address and mask for the VLAN interface.

   For an IPv4 address and mask:

```
# configure vlan Mgmt ipaddress <IPv4 address/mask>
```

   For an IPv6 address and prefix:

```
# configure vlan Mgmt ipaddress <IPv6 address/prefix>
```

4. Add an IP route to the virtual router.

```
# configure iproute add default <gateway> vr VR-Mgmt
```

5. Save the configuration.

```
# save configuration
```

Device Access

You have two options for accessing an EXOS device.

Serial Connection

The serial connection is described in Establish a Serial Connection on page 11. You can close the serial connection by running the **exit** or **logout** command.

SSH

Access the device from a remote client by using the **ssh** command.

Provide the appropriate user credentials to gain access to the device. You can close the session by running the **exit** or **logout** command.

Software Upgrade

Perform the following tasks to upgrade your ExtremeXOS core image and modules.

- Back Up the Configuration on page 13
- Download New Core and Module Images on page 14
- Find the Inactive Partition on page 15
- Install the Core and Module Images on page 16
- Options for Restarting the Switch on page 17

Back Up the Configuration

When you back up the configuration to the database, the switch can reapply the configuration after it is rebooted.

About This Task

The simplest way to back up the configuration is to create a copy of the `Config Booted` file and rename the file with the version number of the new image appended to the file name.

Procedure

1. Save the configuration to the database.

```
# save
```

2. Enter `y` at the prompt to save the configuration.
3. View the `Config Booted` file.

```
# show switch
SysName:          XXXXX
```

```
SysLocation:
SysContact:       support@extremenetworks.com, +1 888 257 3000
System MAC:       00:04:96:51:FE:E2
System Type:      XXXXXX

SysHealth check:  Enabled (Normal)
Recovery Mode:    All
System Watchdog:  Enabled

Current Time:     Sep  4 00:57:18 2022
Timezone:         [Auto DST Disabled] GMT Offset: 0 minutes, name is UTC.
Boot Time:        Sep  3 20:07:11 2022
Boot Count:       402
Next Reboot:      None scheduled
System UpTime:    4 hours 50 minutes 7 seconds

Current State:    OPERATIONAL
Image Selected:   primary
Image Booted:     primary
Primary ver:      x.x.x.x
Secondary ver:    x.x.x.x

Config Selected:  ssh-privatekey.cfg
Config Booted:    ssh-privatekey.cfg
                  ssh-privatekey.cfg Created by ExtremeXOS version
x.x.x.x
            219131 bytes saved on Jul 14 23:03:08 2022
```

4. Copy the `Config Booted` file, appending the version number to the new file name.

```
# cp <old-name> <new-name>
```

For example:

```
# cp ssh-privatekey.cfg ssh-privatekey.cfg-x_x_x_x
```

Download New Core and Module Images

The core image (.xos) file contains the executable code that runs on the switch and is installed at the factory. The module image (.xmod) supplements the core image.

About This Task

The version number of the core image and the module must match. As new versions of this image are released, upgrade both the software and module packages running on your system.

Procedure

1. Obtain the core and module images from the Extreme Networks support site: http://www.extremenetworks.com/support.

   Note
   Access requires a valid user or site ID and a password. If you do not have a Support account, you can request one with the **Request Web Login** link.

2. Place the image files on a server that your switch can locate.

Image Integrity Checking

This feature adds digital signature verification in ExtremeXOS core and module images. Image integrity is checked against the digital signature before actual installation.

Digital Signature

Digital signature is commonly used to demonstrate of the authenticity of a digital message, in this case, the image downloaded to the switch. Only images with digital signature validated on the switch can be installed. Otherwise, the installation will fail.

This feature uses the Public Key Infrastructure (PKI) approach. Specifically, with the RSA algorithm, two keys, the private key and the public key, are generated using the OpenSSL utility. The ExtremeXOS core and module images are digitally signed with the private key. The public key is installed on the switch in the format of a X.509 certificate, which is verified before being used.

The signature is computed for the images when they are built and then included in the final image. During downloading process on the switch, the signature is verified against the image using the installed public key.

For secure delivery, the public key is digitally signed and then distributed in the format of a X.509 certificate. Another set of keys is generated to sign this certificate. A self-signed root certificate is installed on the switch to verify the certificate containing the image signing public key.

All these keys and certificates are generated offline and the private keys should be stored safely.

Transition from an image without a signature to an image with a signature is possible. First, download the ExtremeXOS image and install the public key certificates. At this time, the signature cannot be verified because there is no key to validate the image. But after the first installation, all subsequent downloaded images can be validated using the installed key.

The certificates are included only in the ExtremeXOS core image. XMOD images do not need to include certificates.

Hash Verification

Each ExtremeXOS core and module image is posted with an MD5 (message-digest algorithm 5) hash checksum, which can be verified using any offline tool. A SHA-256 hash checksum is also generated for you to verify offline.

Find the Inactive Partition

A switch can store up to two core images: one active image and one inactive image.

About This Task

You install the software image to the inactive partition and specify that partition while downloading the image to the switch.

Procedure

1. View the `Config Booted` file.

```
# show switch
SysName:          XXXXX
```

```
SysLocation:
SysContact:       support@extremenetworks.com, +1 888 257 3000
System MAC:       00:04:96:51:FE:E2
System Type:      XXXXXX

SysHealth check:  Enabled (Normal)
Recovery Mode:    All
System Watchdog:  Enabled

Current Time:     Sep  4 00:57:18 2022
Timezone:         [Auto DST Disabled] GMT Offset: 0 minutes, name is UTC.
Boot Time:        Sep  3 20:07:11 2022
Boot Count:       402
Next Reboot:      None scheduled
System UpTime:    4 hours 50 minutes 7 seconds

Current State:    OPERATIONAL
Image Selected:   primary
Image Booted:     primary
Primary ver:      x.x.x.x
Secondary ver:    x.x.x.x

Config Selected:  ssh-privatekey.cfg
Config Booted:    ssh-privatekey.cfg
                  ssh-privatekey.cfg Created by ExtremeXOS version
x.x.x.x
            219131 bytes saved on Jul 14 23:03:08 2022
```

2. Locate the **Image Booted** line.

   If the line indicates `primary`, you will install the images on the secondary partition. If it indicates `secondary`, you will install the images on the primary partition.

Install the Core and Module Images

Before You Begin

Ensure that you have downloaded the images to a network server that your switch can locate. For more information, see Download New Core and Module Images on page 14.

Procedure

1. Use one of the following commands to verify the version of the software running on the switch.

   ```
   # show system
   # show version
   ```

2. From the primary node, verify which virtual router reaches your server.

   Use one of the following commands.

   ```
   # ping vr VR-Mgmt <host>
   # ping vr vr-Default <host>
   ```

   At least one of these commands must successfully reach your server for you to download the image. The virtual router that reaches your server is the one that you specify in step 3.

3. Download the core software image.

```
# download image <tftp-server-ipaddress> <image-name.xos>
vr <vr-name> install
```

Note

If you configured the switch to write core dump (debug) files to the internal memory card, you might have insufficient space to complete the image download. If this occurs, move or delete the core dump files from the internal memory. You are asked during the download process if you want to remove these files.

4. When prompted, enter `y` to install the image after download.

   Installation begins.

5. Download the module software image.

```
# download image <tftp-server-ipaddress> <image-name.xmod>
vr <vr-name> install
```

6. When prompted, enter `y` to install the image after download.

   Installation begins.

7. When installation is complete, restart the device.

```
# reboot
```

   For more information, see Options for Restarting the Switch on page 17.

8. Use one of the following commands to verify that the software is upgraded.

```
# show system
# show version
```

Options for Restarting the Switch

- You can restart the switch immediately. Any previously scheduled restart is canceled.

```
# reboot
```

- You can restart the switch at a later time.

```
# reboot {[time <mon> <day> <year> <hour> <min>] | cancel}
{slot <slot-number} {all}
```

  The options use the following formats:

  - date: in mm dd yyy format
  - time: 34-hour clock in hh mm ss format

Tip

Run the **`show switch`** command to see any scheduled restarts.

- You can cancel a scheduled restart by using the **`cancel`** option of the **`reboot`** command.

FIPS Mode

When implemented, Federal Information Processing Standards (FIPS) mode disables some services and disables certain cryptographic, hashing, and signature algorithms that are considered insecure.

For more information, see the Federal Information Processing Standards (FIPS) Mode section of the *ExtremeXOS User Guide*.

Enable FIPS Mode

When FIPS mode is enabled, EXOS uses the `openssl-fips-2.0.16` OpenSSL library.

Procedure

1. Enable FIPS mode.

```
# configure security fips-mode on

FIPS mode will be enabled only after rebooting the switch.
SNMPv3 users configured with either md5 authentication or DES encryption will be
     discarded after reboot.
SSH existing configuration of ciphers/MACs will be lost after reboot.
NTP existing configuration of MD5 authentication type keys will be lost after reboot.
Python scripting configuration is ignored when FIPS mode is 'on'.
#
```

2. Save the changes to non-volatile memory (NVRAM).

```
# save configuration
```

Configuration changes are now saved during reboots and power outages.

3. Reboot the device.

```
# reboot
```

FIPS mode is enabled.

Supported SSH Ciphers and Keys

The following ciphers and keys are claimed or allowed only when the switch is configured in FIPS mode and when certain additional restrictions are configured.

For more information about the additional restrictions, see Restrict SSH Algorithms and Keys on page 45.

Encryption ciphers

- AES-128-CBC
- AES-256-CBC
- AES-128-CTR
- AES-256-CTR

SSH public key

SSH-RSA

MAC ciphers

- HMAC-SHA1

- HMAC-SHA2-256
- HMAC-SHA2-512

Key exchange methods

- Diffie-Hellman-Group14-SHA1
- Diffie-Hellman-Group14-SHA256
- Diffie-Hellman-Group16-SHA512
- Diffie-Hellman-Group18-SHA512

Supported TLS Ciphers and Curves

The following ciphers and curves are claimed or allowed only when the switch is configured in FIPS mode.

Ciphers

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- 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

Curves

The switch supports the following curves, which are presented in the Elliptic Curves/Groups Extension in the client Hello.

- secp256r1
- secp384r1
- secp521r1

Change the Passwords for the Default Accounts

By default, an EXOS device is configured with two accounts: `admin` and `user`.

Before You Begin

Only a valid administrator with the `admin` role can perform this task.

About This Task

The default password for each account is null, meaning there is no password. Take the following steps to change the password.

Note

Passwords can have a maximum of 32 characters and are case-sensitive.

Procedure

1. Change the password for the admin account.

```
# configure account admin
Current password:
Password: <new-password>
Reenter password: <new-password>
```

2. Change the password for the user account.

```
# configure account user
Current password:
Password: <new-password>
Reenter password: <new-password>
```

Create a Failsafe Account

A failsafe account provides access to the device if the other accounts cannot be used. It is your last resort for accessing a device.

About This Task

The failsafe account is always present on the device but is never displayed by the **show accounts** command. The failsafe account has administrator access privileges.

The following procedure describes how to set the user name and password for the failsafe account. However, you can also use the **configure failsafe-account** command to restrict access to specified connection types, such as serial and SSH. For more information, see the ExtremeXOS Command Reference Guide.

Procedure

1. Configure the user name and password.

```
# configure failsafe-account

Enter failsafe user name: <username>
Enter failsafe password: <password>
Enter password again: <password>
```

2. To display the configured user name, password, or access restrictions, run the following command.

```
# show failsafe-account
```

Set the System Date, Time, and Time Zone

You can manually configure the date, time, and time zone.

About This Task

You can also synchronize a device with an external Network Time Protocol (NTP) server. For more information, see Network Time Protocol on page 53.

Note

As a best practice, do not update the time manually when NTP is enabled.

Procedure

1. Log in to the device as an administrator.
2. Configure the date and time in the following format: month, day, year, hour, minutes, seconds.

```
# configure time <month> <day> <year> <hour> <min> <sec>
```

3. Configure the time zone to use an internal system clock to maintain accurate time.

```
# configure timezone name <time-zone-name> <GMT-offset-in-minutes>
{autodst {name <dst-timezone-ID>} {<dst-offset>} {begins [every <floatingday> |
on <absoluteday>] {at <time-of-day>} {ends [every <floatingday> | on <absoluteday>]
{at <time-of-day>}}} | noautodst}
```

The following example configures the time zone for the area of NY, NY America and sets Daylight Saving Time.

```
# configure timezone name EDT -300 autodst begins every second Sunday
march at 2 00 ends every first Sunday November at 2 00 name EST +60
```

Audit Logs and Syslog

The transmission of audit logs to the external audit (syslog) server occurs in real time, with each audit record transferred as it is generated.

If the connection to the external audit server is lost, the EXOS switch continues to save local audit logs so there is no loss of audit. An automated log reconciliation process (syncing) occurs between the locally stored records with the external audit server when the connection is reestablished.

You cannot directly access the stored audit records, but you can use the CLI to display the logs.

Log Filters

EXOS provides configurable audit filters, including a global filter (DefaultFilter) that defines the default audit behavior for all targets. The primary command for configuring filters is **`configure log filter events match`**.

For more information, see Configure Log Filters on page 23 and the ExtremeXOS Command Reference Guide.

Log Records

The system logs audit records for events, administrative actions, protocols, and management functions. For more information, see Audit Record Samples on page 25.

For each captured audit, the generated record contains the date, time, and type of event, the subject identity (for example, IP Address or User Name), the outcome, and the severity of the event.

Log Severity Levels

Audit log records are categorized into several severity levels, as shown in the following table. By default, the memory-buffer and syslog targets are configured to capture log information at the debug-data level through the critical level.

Severity Level	Description
Critical, code 2	A serious problem that compromises the operation of the system. The system cannot function as expected unless the situation is remedied, such as resetting the device.
Error, code 3	A problem that interferes with the normal operation of the system. The system is not functioning as expected.
Warning, code 4	An abnormal condition that does not interfere with the normal operation of the system. This condition indicates that the system or the network in general might not function as expected.
Notice, code 5	A normal but significant condition, which signals that the system is functioning as expected.
Info, code 6	A normal but potentially interesting condition, which signals that the system is functioning as expected. This level simply provides details.
Debug-Verbose, code 7	A condition of possible interest to a developer who is analyzing some system behavior at a more verbose level than provided by the debug summary information.

Enable a TLS Connection to the Syslog Server

EXOS communicates with an external syslog (audit) server by establishing a trusted channel between itself and the syslog server.

About This Task

Implementation of the trusted channel uses TLS v1.2 with server-side X.509v3 certificate-based authentication, in which the X.509v3 certificate that the syslog server presents is checked against the configured trusted CA (certificate authority) chain and validated by the Online Certificate Status Protocol (OCSP). For more information, see X.509 Certificate-Based Authentication on page 47 and Reconnect a TLS Session on page 51.

Mutual authentication is also supported.

When the switch is configured in FIPS mode, only the claimed or allowed TLS ciphers are available. For more information, see Supported TLS Ciphers and Curves on page 19.

Take the following steps to enable a TLS connection to the syslog server. For explanations and examples of the commands, see the ExtremeXOS Command Reference Guide.

Procedure

1. Enable the OCSP validation for TLS.

```
# configure syslog tls ocsp on
```

2. Configure the remote syslog server host address.

```
# configure syslog add <ip-addr> tls-port <port-num>
vr <virtual-router-name> [local0...local7]
```

3. Specify the remote syslog server certificate reference identifier.

```
# configure syslog <ip-addr> tls-port <port-num> vr <virtual-router-name>
[local0...local7] reference-identifier <ID>
```

4. Enable the log target.

```
# enable log target syslog <ip-addr> tls-port <port-num>
vr <virtual-router-name> [local0...local7]
```

5. Configure the filter and the severity level for the log target.

```
# configure log target syslog <ip-addr> tls-port <port-num>
vr <virtual-router-name> [local0...local7] filter <filter-name>
severity <severity-level>
```

6. Associate any match expression with the log target.

```
# configure log target syslog <ip-addr> tls-port <port-num>
vr <virtual-router-name> [local0...local7] match Any
```

7. Configure the format of messages for the log target.

```
# configure log target syslog <ip-addr> tls-port <port-num>
vr <virtual-router-name> [local0...local7] format [timestamp [ seconds|hundredths|
none]]
[date [ dd-Mmm-yyyy|yyyy-mm-dd|Mmm-dd|mm-dd-yyyy|mm/dd/yyyy|dd-mm-yyyy|none]]
{event-name [component|condition| none]} {severity} {priority} {host-name}
{source-line} {tag-id} {tag-name}
```

8. Enable logging to all remote syslog host targets.

```
# enable syslog
```

Enable CLI Logging to Syslog

You can record all configuration changes that are made from the command-line interface (CLI).

About This Task

The changes are logged to the system log. Configuration logging applies only to commands that result in a configuration change.

Procedure

Enable CLI logging.

```
# enable cli-config-logging
```

Configure Log Filters

You can configure different filters for each target.

About This Task

A global filter, DefaultFilter, defines the default audit behavior for all targets. The following steps offer examples of the types of filters you can configure. For more information about the commands, see the ExtremeXOS Command Reference Guide.

Procedure

1. To enable debug mode, run the following command.

```
# enable log debug-mode
```

2. To enable only users with administrative privileges to view logs, run the following command.

```
# configure log messages privilege admin
```

3. To add THTTPD events to the DefaultFilter, with a minimum severity level of info, run the following command.

```
# configure log filter DefaultFilter add events thttpd
severity info
```

4. To add EXSSHD events to the DefaultFilter, with a minimum severity level of debug-verbose, run the following command.

```
# configure log filter DefaultFilter add events exsshd
severity debug-verbose
```

5. To add CM events to the DefaultFilter, with a minimum severity level of debug-verbose, run the following command.

```
# configure log filter DefaultFilter add events cm
severity debug-verbose
```

6. To add AAA events to the DefaultFilter, with a minimum severity level of debug-verbose, run the following command.

```
# configure log filter DefaultFilter add events aaa
severity debug-verbose
```

Configure the Size of the Logging Buffer

You can configure the size of the local buffer, from 200 to 20000 log messages.

About This Task

When the buffer is full, the oldest message is overwritten first, a process commonly called FIFO (First In, First Out).

Procedure

1. Specify the number of messages that can be in the memory buffer before the oldest message is overwritten.

```
# configure log target memory-buffer number-of-messages 200
```

In this example, the size of the buffer is set to 200 messages. Note that the local memory buffer is deleted when the switch is restarted.

2. (Optional) View the messages that are stored in the memory buffer.

```
# show log messages memory-buffer {starting [date <date>
time <time>]} {ending [date <date>
time <time>]}
```

You can use the optional **starting** and **ending** parameters to find messages from a specific period.

3. (Optional) View the messages that are stored in NVRAM.

```
# show log messages nvram {starting [date <date>
time <time>]} {ending [date <date>
time <time>]}
```

You can use the optional **starting** and **ending** parameters to find messages from a specific period.

Note
The NVRAM storage limit is 20 KB. When that limit is reached, the oldest messages are overwritten.

Self-Test Audit Log Records

Self-tests are performed during start-up of the switch and audit records are generated for successful and failed tests.

These self-tests, which consist of known-answer algorithm testing and integrity testing, comply with FIPS 140-2 requirements for self-testing. The tests cover all anticipated modes of failure. Failure of any self-test during the start-up process stops the process and prompts you to reload.

The following is an example of a log entry for a successful self-test.

```
08/14/2021 14:17:49.99 <Noti:SNMP.Major.EnblFIPSModeOK> Self-Test passed.
FIPS mode enabled.
```

The following is an example of a log entry for a failed self-test.

```
06/13/2021 13:46:29.61 <Erro:exsshd.EnblFIPSModeFail> Failed to enable FIPS
mode: error:2D080086:lib(45):func(128):reason(134)
```

Note
When some low-level critical failure modes prevent the switch from starting up, audit records are not generated. In such cases, the switch enters a failure mode and displays error codes, typically on the console. You can configure the switch to reboot or to stop, with errors displayed, when non-critical errors are encountered. The cryptographic module performs self-tests during start-up. Messages from the module are displayed on the console and audit records are generated for both successful and failed tests.

Audit Record Samples

This topic provides an example of the audit records for each auditable event.

The following table pairs the text of the audit records from the X440-G2 switch with the corresponding requirement identifier and feature. The record text is the same for all claimed devices in the

evaluated configuration. For more information about claimed devices, see Common Criteria Certification Configuration on page 10.

Table 1: Audit Record Samples

Requirement Identifier	Feature	Audit Record Text
FAU_GEN.1	Start and stop of audit functions	<189> 2022-02-19 05:37:15 x440 log: The Event Management System logging server has started.
FAU_GEN.1	Start and stop of audit functions	<190> 2022-02-19 05:36:01 x440 cli: serial testadmin: reboot.
FAU_GEN.1	Start and stop of audit functions	<188> 2022-02-19 05:36:03 x440 EPM: User testadmin: Rebooting with reason User requested switch reboot.
FCS_NTP_EXT.1	Add and remove time server	<190> 2022-02-21 17:14:00 x440 cli: serial admin: configure ntp server add 192.0.2.0 key 2 vr VR-Mgmt.
FCS_NTP_EXT.1	Add and remove time server	<190> 2022-02-21 17:05:57 x440 cli: serial admin: configure ntp server delete 192.0.2.0.
FCS_SSHS_EXT.1	Failure to establish SSH session	<189> 2022-07-19 04:15:25 x440 exsshd: SSH connection from source 192.0.2.0 port 43444 has been denied due to key exchange failed : no matching cipher found. Client offer: aes128-gcm@openssh.com.
FCS_SSHS_EXT.1	Failure to establish SSH session	<189> 2022-07-19 04:18:20 x440 exsshd: SSH connection from source 192.0.2.0 port 43788 has been denied due to key exchange failed : no matching host key type found. Client offer: rsa-sha2-256.
FCS_SSHS_EXT.1	Failure to establish SSH session	<189> 2022-07-19 04:24:21 x440 exsshd: SSH connection from source 192.0.2.0 port 44400 has been denied due to key exchange failed : no matching MAC found. Client offer: hmac-md5.
FCS_SSHS_EXT.1	Failure to establish SSH session	<189> 2022-07-19 04:28:05 x440 exsshd: SSH connection from source 192.0.2.0 port 44744 has been denied due to key exchange failed : no matching key exchange method found. Client offer: diffie-hellman-group1-sha1,ext-info-c.

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FCS_SSHS_EXT.1	SSH session termination	<189> 2022-04-15 03:29:31 x440 exsshd: Terminated the connection with user admin 192.0.2.0 port 38792 due to receiving a bad packet of length 262156.
FCS_SSHS_EXT.1	SSH rekeying for time and volume	<191> 2022-07-19 04:37:11 x440 exsshd: SSH Rekeying.
FCS_TLSC_EXT.1	Missing server authentication	<187> 2022-03-08 20:05:42 x440 log: Syslog SSL certificate verification error: 26 (unsupported certificate purpose)#012Certificate at depth: 0#012Issuer: /C=US/ ST=MD/L=Catonsville/O=GSS/ CN=subsubca-rsa/ emailAddress=subsubca-rsa@mycompany.com#012Subject: /C=US/ST=MD/L=Catonsville/ O=GSS/ CN=tl27-16x.mycompany.com/ emailAddress=server-no-auth-eku-rsa@mycompany.com.
FCS_TLSC_EXT.1	Missing server authentication	<187> 2022-03-08 20:05:42 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed".
FCS_TLSC_EXT.1	Wrong certificate type	<187> 2022-03-08 20:11:37 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:1409017F:SSL routines:ssl3_get_server_certificate:wrong certificate type".
FCS_TLSC_EXT.1	Bad signature	<187> 2022-03-08 20:46:36 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:04097068:rsa routines:RSA_private_encrypt:bad signature".

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FCS_TLSC_EXT.1	Bad curve	<187> 2022-04-15 21:56:44 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:1408D17A:SSL routines:ssl3_get_key_exchange: wrong curve".
FCS_TLSC_EXT.1	Unknown cipher	<187> 2022-03-08 20:16:37 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:140920F8:SSL routines:ssl3_get_server_hello:unknown cipher returned".
FCS_TLSC_EXT.1	Wrong TLS version	<187> 2022-03-08 20:41:36 x440 log: Syslog SSL connection(192.168.144.254:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:1409210A:SSL routines:ssl3_get_server_hello:wrong ssl version".
FCS_TLSC_EXT.1	Handshake error	<187> 2022-03-07 20:36:16 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure".
FCS_TLSC_EXT.1	Modified finished message	<187> 2022-03-08 20:51:36 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:1408C095:SSL routines:ssl3_get_finished:digest check failed".
FCS_TLSC_EXT.1	Plaintext finished message	<187> 2022-03-08 20:56:37 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:1408F081:SSL routines:SSL3_GET_RECORD:block cipher pad is wrong".

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FCS_TLSC_EXT.1	Bad reference identifier	<187> 2022-03-08 22:24:02 x440 log: Syslog SSL certificate verification error: 62 (Hostname mismatch)#012Certificate at depth: 0#012Issuer: /C=US/ST=MD/L=Catonsville/O=GSS/CN=subsubca-rsa/emailAddress=subsubca-rsa@mycompany.com#012Subject: /C=US/ST=MD/L=Catonsville/O=GSS/CN=Completely Random Common Name (Bad CN identifier)/emailAddress=server-san-none-cn-bad-dns-rsa@mycompany.com.
FCS_TLSC_EXT.1	Bad reference identifier	<187> 2022-03-08 22:24:02 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed".
FIA_AFL.1	Failed login	<188> 2022-02-08 00:32:26 x440 AAA: Login failed due to invalid username/password for user testadmin through ssh (192.0.2.0).
FIA_AFL.1	Failed login	<188> 2022-02-08 00:32:26 x440 AAA: Account for user 'testadmin' locked out!
FIA_UAU_EXT.2	Identification and authentication mechanism	See FIA_UIA_EXT.1.
FIA_UIA_EXT.1	Successful console login	<190> 2022-03-10 19:59:51 x440 AAA: Login passed for user admin through serial.
FIA_UIA_EXT.1	Failed console login	<180> 2022-03-10 19:59:45 x440 AAA: Login failed due to invalid username/password for user through serial.
FIA_UIA_EXT.1	Successful SSH or CLI login	<182> 2022-03-10 18:28:47 x440 AAA: Login passed for user admin through ssh (192.0.2.0).
FIA_UIA_EXT.1	Failed SSH or CLI login	<188> 2022-02-08 00:39:53 x440 AAA: Login failed due to invalid username/password for user testadmin through ssh (192.0.2.0).

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FIA_UIA_EXT.1	Successful SSH or CLI login (public key)	<190> 2022-01-18 23:43:16 x440 AAA: Msg from Master : Found valid key for user admin.
FIA_UIA_EXT.1	Successful SSH or CLI login (public key)	<190> 2022-01-18 23:43:16 x440 AAA: Msg from Master : Login passed for user admin through ssh (192.0.2.0).
FIA_UIA_EXT.1	Successful SSH or CLI login (public key)	<190> 2022-01-18 23:43:16 x440 AAA: Msg from Master : Did key authentication for user admin (192.0.2.0).
FIA_UIA_EXT.1	Failed SSH or CLI login (public key)	<188> 2022-03-10 18:28:47 x440 exsshd: Key authentication failed for user admin from 192.0.2.0. Key invalid/not configured to the user.
FIA_X509_EXT.1/Rev	Add trust anchor	2021-12-10T15:07:12.232106-05:0 0 x440 cli:192.0.2.0 (ssh) admin: download ssl 192.0.2.0 certificate trusted-ca rootca-rsa.pem.
FIA_X509_EXT.1/Rev	Add trust anchor	2021-12-10T15:07:12.265745-05:0 0 x440 thttpd: The provided CA certificate (CN:rootca-rsa) is valid.
FIA_X509_EXT.1/Rev	Remove trust anchor	<190> 2022-07-19 03:52:39 x440 cli: serial admin: unconfigure ssl certificate trusted-ca subca-rsa.pem.
FIA_X509_EXT.1/Rev	Remove trust anchor	<189> 2022-07-19 03:52:39 x440 thttpd: The specified CA certificate (CN:subca-rsa) has been unconfigured successfully.
FIA_X509_EXT.1/Rev	Missing basic constraints	<187> 2022-04-15 07:41:24 x440 log: Syslog SSL certificate verification error: 24 (invalid CA certificate) depth: 1 issuer: / C=US/ST=MD/L=Catonsville/ O=GSS/CN=subca-rsa/ emailAddress=subca-rsa@mycompany.com subject: / C=US/ST=MD/L=Catonsville/ O=GSS/CN=subsubca-no-basic-constraints-rsa/ emailAddress=subsubca-no-basic-constraints-rsa@mycompany.com.

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FIA_X509_EXT.1/Rev	Missing basic constraints	<187> 2022-04-15 07:41:24 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed".
FIA_X509_EXT.1/Rev	Basic constraints false for CA	<187> 2022-05-30 18:39:34 x440 log: Syslog SSL certificate verification error: 24 (invalid CA certificate) depth: 1 issuer: /C=US/ST=MD/L=Catonsville/O=GSS/CN=subca-rsa/emailAddress=subca-rsa@mycompany.com subject: /C=US/ST=MD/L=Catonsville/O=GSS/CN=subsubca-ca-flag-false-rsa/emailAddress=subsubca-ca-flag-false-rsa@mycompany.com.
FIA_X509_EXT.1/Rev	Basic constraints false for CA	<187> 2022-05-30 18:39:34 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed".
FIA_X509_EXT.1/Rev	Certificate revoked	<187> 2022-05-27 19:55:06 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: OCSP revocation check failed at depth 0 subject /C=US/ST=MD/L=Catonsville/O=GSS/CN=tl27-16x.mycompany.com/emailAddress=server-revoked-rsa@mycompany.com. OCSP_RevocationCheck() returned "OCSP Response - Leaf certificate is revoked".

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FIA_X509_EXT.1/Rev	Certificate revoked	<187> 2022-05-27 20:06:08 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: OCSP revocation check failed at depth 2 subject / C=US/ST=MD/L=Catonsville/ O=GSS/CN=subca-revoked-rsa/ emailAddress=subca-revoked-rsa@mycompany.com. OCSP_RevocationCheck() returned "OCSP Response - Certificate of intermediate CA in chain is revoked".
FIA_X509_EXT.1/Rev	Certificate revoked	<187> 2022-05-27 20:14:21 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: OCSP revocation check failed at depth 2 subject / C=US/ST=MD/L=Catonsville/ O=GSS/CN=subca-rsa/ emailAddress=subca-rsa@mycompany.com. OCSP_RevocationCheck() returned "OCSP Response basic verification failed".
FIA_X509_EXT.1/Rev	Corrupt certificate ASN1	<187> 2022-05-18 20:14:38 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag".
FIA_X509_EXT.1/Rev	Corrupt certificate signature	<187> 2022-05-27 21:20:36 x440 log: Syslog SSL certificate verification error: 7 (certificate signature failure) depth: 0 issuer: / C=US/ST=MD/L=Catonsville/ O=GSS/CN=subsubca-rsa/ emailAddress=subsubca-rsa@mycompany.com subject: /C=US/ST=MD/ L=Catonsville/O=GSS/ CN=tl27-16x.mycompany.com/ emailAddress=server-rsa@mycompany.com

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FIA_X509_EXT.1/Rev	Corrupt certificate signature	<187> 2022-05-27 21:20:36 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:0407006A:rsa routines:RSA_padding_check_PKCS1_type_1:block type is not 01".
FIA_X509_EXT.1/Rev	Corrupt public key	<187> 2022-05-27 21:25:36 x440 log: Syslog SSL certificate verification error: 7 (certificate signature failure) depth: 0 issuer: /C=US/ST=MD/L=Catonsville/O=GSS/CN=subsubca-rsa/emailAddress=subsubca-rsa@mycompany.com subject: /C=US/ST=MD/L=Catonsville/O=GSS/CN=tl27-16x.mycompany.com/emailAddress=server-rsa@mycompany.com.
FIA_X509_EXT.1/Rev	Corrupt public key	<187> 2022-05-27 21:25:36 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:04097068:rsa routines:RSA_private_encrypt:bad signature".
FIA_X509_EXT.1/Rev	Invalid chain	<187> 2022-05-30 18:26:56 x440 log: Syslog SSL certificate verification error: 19 (self signed certificate in certificate chain) depth: 1 issuer: /C=US/ST=MD/L=Catonsville/O=GSS/emailAddress=rootca-unacceptable-rsa@mycompany.com/CN=rootca-unacceptable-rsa subject: /C=US/ST=MD/L=Catonsville/O=GSS/emailAddress=rootca-unacceptable-rsa@mycompany.com/CN=rootca-unacceptable-rsa.

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FIA_X509_EXT.1/Rev	Invalid chain	<187> 2022-05-30 18:26:56 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed".
FIA_X509_EXT.1/Rev	Unreachable revocation server	<187> 2022-05-30 18:46:56 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: OCSP revocation check failed at depth 0 subject /C=US/ST=MD/L=Catonsville/O=GSS/CN=tl27-16x.mycompany.com/emailAddress=server-unreachable-revocation-rsa@mycompany.com. OCSP_RevocationCheck() returned "No valid URIs present in AIA".
FIA_X509_EXT.1/Rev	Expired certificate	<187> 2022-05-27 19:09:49 x440 log: Syslog SSL certificate verification error: 10 (certificate has expired) depth: 0 issuer: /C=US/ST=MD/L=Catonsville/O=GSS/CN=subsubca-rsa/emailAddress=subsubca-rsa@mycompany.com subject: /C=US/ST=MD/L=Catonsville/O=GSS/CN=tl27-16x.mycompany.com/emailAddress=server-expired-rsa@mycompany.com.
FIA_X509_EXT.1/Rev	Expired certificate	<187> 2022-05-27 19:09:49 x440 log: Syslog SSL connection (192.0.2.0:6514) failed: Can't connect to syslog server with SSL. SSL_connect() returned "error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed".
FMT_MOF.1/ManualUpdate	Manual update attempts	See FMT_SMF.1.
FMT_SMF.1	Local and remote system administration	See FIA_UIA_EXT.1.
FMT_SMF.1	Access banner	<190> 2022-07-19 05:31:32 x440 cli: serial admin: configure banner before-login.

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FMT_SMF.1	Access banner	<190> 2022-07-19 05:32:00 x440 cli: serial admin: configure banner after-login.
FMT_SMF.1	Session inactivity configuration	<190> 2022-02-11 03:35:25 x440 cli: 192.0.2.0 (ssh) admin: configure ssh2 idletimeout 1.
FMT_SMF.1	Session inactivity configuration	<190> 2022-02-15 18:37:34 x440 cli: serial admin: configure cli idle-timeout 1.
FMT_SMF.1	System update and verification	<190> 2022-05-25 18:20:37 x440 cli: serial admin: download image 192.0.2.0 summitX-31.3.100.18.xos VR 0.
FMT_SMF.1	System update and verification	<189> 2022-05-25 18:20:43 x440 EPM. Upgrade: User admin: Download image from hostname IP address192.0.2.0 file name summitX-31.3.100.18.xos VR VR-Mgmt.
FMT_SMF.1	System update and verification	<189> 2022-05-25 18:21:24 x440 EPM: User admin: Download of image finished with status success; Image integrity check passed.
FMT_SMF.1	System update and verification	<189> 2022-05-25 18:21:24 x440 EPM. Upgrade: User admin: Image upgrade has started.
FMT_SMF.1	System update and verification	<189> 2022-05-25 18:23:40 x440 EPM: User admin: Image installation finished with status success.
FMT_SMF.1	Authentication failure configuration	<190> 2022-02-08 00:20:11 x440 cli: serial admin: configure account testadmin password-policy lockout-on-login-failures on.
FMT_SMF.1	Authentication failure configuration	<190> 2022-02-08 00:20:11 x440 AAA: User 'admin' modified lockout allowed setting for 'testadmin' users.
FMT_SMF.1	Authentication failure configuration	<190> 2022-02-08 00:20:39 x440 cli: serial admin: configure account testadmin password-policy lockout-time-period 1.

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FMT_SMF.1	Authentication failure configuration	<190> 2022-02-08 00:20:39 x440 AAA: User 'admin' modified lockout time period setting for 'testadmin' users.
FMT_SMF.1	Authentication failure configuration	<190> 2022-02-08 00:20:51 x440 cli: serial admin: configure cli max-failed-logins 3.
FMT_SMF.1	Audit data transmission behavior	<190> 2022-07-19 05:52:34 x440 cli: serial admin: configure syslog add 192.0.2.0 tls-port 6514 vr VR-Mgmt local6.
FMT_SMF.1	Audit data transmission behavior	<190> 2022-07-19 05:53:37 x440 cli: serial admin: configure syslog 192.0.2.0 tls-port 6514 vr VR-Mgmt local6 reference-identifier tl27-16x.mycompany.com.
FMT_SMF.1	Audit data transmission behavior	<190> 2022-07-19 05:52:52 x440 cli: serial admin: configure log target syslog 192.0.2.0 tls-port 6514 vr VR-Mgmt local6 filter DefaultFilter severity debug-data.
FMT_SMF.1	Audit data transmission behavior	<190> 2022-07-19 05:53:08 x440 cli: serial admin: configure log target syslog 192.0.2.0 tls-port 6514 vr VR-Mgmt local6 match any.
FMT_SMF.1	Audit data transmission behavior	<190> 2022-07-19 05:53:23 x440 cli: serial admin: configure log target syslog 192.0.2.0 tls-port vr VR-Mgmt local6 format timestamp seconds date yyyy-mm-dd event-name none priority host-name tag-name.
FMT_SMF.1	Audit data transmission behavior	<190> 2022-07-02 00:38:29 x440 cli: serial admin: enable log target syslog 192.0.2.0 tls-port 6514 vr VR-Mgmt local6.
FMT_SMF.1	Cryptographic key management	<190> 2022-01-18 23:30:07 x440 cli: serial admin: configure sshd2 user-key admin_rsa_pubkey2 add user admin

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FMT_SMF.1	Cryptographic key management	<189> 2022-01-18 23:30:07 x440 exsshd: Bind user admin to SSH public key admin_rsa_pubkey2 of SHA256 fingerprint 16:27:01:70:2b:c7:14:41:84:55:f6:f7 :bb:3f:30:09:20:e3:f3:7c: d2:03:f6:3c:3b:72:4e:a5:9f:7e:da:1 1 successfully.
FMT_SMF.1	Cryptographic key management	<190> 2022-03-07 20:07:12 x440 cli: serial admin: configure syslog tls ocsp on.
FMT_SMF.1	Cryptographic key management	<190> 2022-01-14 18:23:49 x440 cli: 192.0.2.0 (ssh) admin: configure syslog tls cipher all on.
FMT_SMF.1	Cryptographic key management	2021-12-09T15:25:02.580498-05: 00 x440 cli: 192.0.2.0 (ssh) admin: configure ssl csr privkeylen 2048 country US organization GSS common-name SyslogClientRSA.
FMT_SMF.1	Cryptographic key management	2021-12-09T15:25:27.525388-05: 00 x440 thttpd: Creating CSR with key length: 2048, country code: US, organization: GSS, CN: SyslogClientRSA.
FMT_SMF.1	Cryptographic key management	2021-11-30T10:49:40.546333-05: 00 x440 cli: 192.0.2.0 (ssh) admin: configure ssh2 enable pk-alg ssh-rsa.
FMT_SMF.1	Cryptographic key management	2021-11-30T10:52:09.358517-05:0 0 x440 cli: 192.0.2.0 (ssh) admin: configure ssh2 disable pk-alg x509v3-sign-dss.
FMT_SMF.1	Cryptographic key management	2021-11-30T10:57:33.323841-05:0 0 x440 cli: 192.0.2.0 (ssh) admin: configure ssh2 dh-group minimum 14.
FMT_SMF.1	SSH rekeying thresholds	<190> 2022-07-19 03:36:27 x440 cli: serial admin: configure ssh2 rekey time-interval 15.
FMT_SMF.1	SSH rekeying thresholds	<190> 2022-07-19 03:36:49 x440 cli: serial admin: configure ssh2 rekey data-limit 1.
FMT_SMF.1	TImestamp configuration	See FPT_STM_EXT.1

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FMT_SMF.1	Password reset	<190> 2022-02-17 20:23:53 x440 AAA: User 'admin' changed password for user 'testadmin2' successfully.
FMT_SMF.1	NTP configuration	See FPT_NTP_EXT.1
FMT_SMF.1	Reference identifier configuration	2021-12-13T19:26:55.527917-05:00 x440 cli: serial admin: configure syslog 192.0.2.0 tls-port 6514 vr VR-Mgmt local6 reference-identifier tl27-16x.mycompany.com.
FMT_SMF.1	Trust store and public key management	2021-12-10T15:07:12.232106-05:00 x440 cli: 192.0.2.0 (ssh) admin: download ssl 192.0.2.0 certificate trusted-ca rootca-rsa.pem.
FMT_SMF.1	Trust store and public key management	2021-12-10T15:07:12.265745-05:00 x440 thttpd: The provided CA certificate (CN:rootca-rsa) is valid.
FMT_SMF.1	Trust store and public key management	<190> 2022-07-19 03:52:39 x440 cli: serial admin: unconfigure ssl certificate trusted-ca subca-rsa.pem.
FMT_SMF.1	Trust store and public key management	<189> 2022-07-19 03:52:39 x440 thttpd: The specified CA certificate (CN:subca-rsa) has been unconfigured successfully.
FMT_SMF.1	Trusted public key management	<190> 2022-07-19 02:07:13 x440 cli: 192.0.2.0 (ssh) admin: configure sshd2 user-key admin_rsa_pubkey2 add user admin
FMT_SMF.1	Trusted public key management	<190> 2022-03-04 05:55:43 x440 cli: serial admin: delete sshd2 user-key admin_rsa_pubkey2
FMT_SMF.1	X509v3 certificate import	2021-12-10T15:07:12.232106-05:00 x440 cli: 192.0.2.0 (ssh) admin: download ssl 192.0.2.0 certificate trusted-ca rootca-rsa.pem.
FMT_SMF.1	X509v3 certificate import	2021-12-10T15:07:12.265745-05:00 x440 thttpd: The provided CA certificate (CN:rootca-rsa) is valid.

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FMT_SMF.1	X509v3 certificate import	2021-12-09T15:25:02.580498-05:00 x440 cli: 192.0.2.0 (ssh) admin: configure ssl csr privkeylen 2048 country US organization GSS common-name SyslogClientRSA.
FMT_SMF.1	X509v3 certificate import	2021-12-09T15:25:27.525388-05:00 x440 thttpd: Creating CSR with key length: 2048, country code: US, organization: GSS, CN: SyslogClientRSA.
FMT_SMF.1	X509v3 certificate import	2021-12-10T15:12:56.540483-05:00 x440 cli: 192.0.2.0 (ssh) admin: download ssl 192.0.2.0 certificate csr-cert server-x440-rsa.pem.
FMT_SMF.1	X509v3 certificate import	2021-12-10T15:12:56.573803-05:00 x440 thttpd: The provided SSL certificate (CN:SyslogClientRSA) is valid.
FMT_SMF.1	X509v3 certificate import	2021-12-10T15:12:56.576196-05:00 x440 thttpd: SSL private key and SSL certificate (CN:SyslogClientRSA) matches.
FPT_STM_EXT.1	Discontinuous time changes	Manual time change: <190> 2022-04-15 05:01:28 x440 cli: serial admin: configure time 4 15 2022 5 6 15 .
FPT_STM_EXT.1	Discontinuous time changes	Manual time change: <189> 2022-04-15 05:01:28 x440 DM: Setting time from Fri Apr 15 05:01:28 2022 to Fri Apr 15 05:06:15 2022.
FPT_STM_EXT.1	Discontinuous time changes	NTP time change: <189> 2022-06-08 17:55:53 x440 NTP. Peer: The NTP server 192.0.2.0 is selected as system peer.
FPT_STM_EXT.1	Discontinuous time changes	NTP time change: <190> 2022-06-08 17:55:53 x440 NTP. Sys: Clock step -778.895724 seconds was detected and the system clock is updated.
FPT_STM_EXT.1	Discontinuous time changes	NTP time change: <190> 2022-06-08 17:55:53 x440 NTP. Sys: Changing the system time from Wed Jun 8 17:55:53 2022 to Wed Jun 8 17:42:54 2022 due to a clock step event.

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FPT_TUD_EXT.1	Success and failure of update attempts	Success: <190> 2022-05-25 18:20:37 x440 cli: serial admin: download image 192.0.2.0 summitX-31.3.100.18.xos VR 0.
FPT_TUD_EXT.1	Success and failure of update attempts	Success: <189> 2022-05-25 18:20:43 x440 EPM. Upgrade: User admin: Download image from hostname IP address 192.0.2.0 file name summitX-31.3.100.18.xos VR VR-Mgmt.
FPT_TUD_EXT.1	Success and failure of update attempts	Success: <189> 2022-05-25 18:21:24 x440 EPM: User admin: Download of image finished with status success; Image integrity check passed.
FPT_TUD_EXT.1	Success and failure of update attempts	Success: <189> 2022-05-25 18:21:24 x440 EPM. Upgrade: User admin: Image upgrade has started.
FPT_TUD_EXT.1	Success and failure of update attempts	Success: <189> 2022-05-25 18:23:40 x440 EPM: User admin: Image installation finished with status success.
FPT_TUD_EXT.1	Success and failure of update attempts	Failure: <190> 2022-02-07 22:29:32 x440 cli: serial admin: download image 192.0.2.0 summitX-31.3.100.7_corrupt.xos VR.
FPT_TUD_EXT.1	Success and failure of update attempts	Failure: <189> 2022-02-07 22:29:36 x440 EPM. Upgrade: User admin: Download image from hostname IP address 192.0.2.0 file name summitX-31.3.100.7_corrupt.xos VR VR-Mgmt.
FPT_TUD_EXT.1	Success and failure of update attempts	Failure: <187> 2022-02-07 22:29:57 x440 EPM. Upgrade: Upgrade failed, script: Cannot validate image.
FPT_TUD_EXT.1	Success and failure of update attempts	Failure: <189> 2022-02-07 22:29:57 x440 EPM: User admin: Download of image finished with status failure - Image signature cannot be validated.
FTA_SSL.3	Remote session termination	<190> 2022-02-11 03:36:38 x440 AAA: Administrative account (admin) logout from ssh (192.0.2.0).

Table 1: Audit Record Samples (continued)

Requirement Identifier	Feature	Audit Record Text
FTA_SSL.3	Remote session termination	<191> 2022-02-11 03:36:38 x440 exsshd: Session closed on ssh idle timeout.
FTA_SSL4	Interactive session termination	SSH: <190> 2022-07-19 02:09:23 x440 AAA: Administrative account (admin) logout from ssh (192.0.2.0).
FTA_SSL4	Interactive session termination	Local console: <190> 2022-07-19 02:00:46 x440 AAA: Administrative account (admin) logout from serial.
FTA_SSL_EXT.1	Local session termination	<190> 2022-02-15 18:38:51 x440 AAA: Administrative account (admin) logout from serial.
FTP_ITC.1	TLS client session establishment	<181> 2022-03-08 18:36:34 x440 log: Syslog SSL connection (192.0.2.0:6514) established.
FTP_ITC.1	TLS client session termination	<187> 2022-03-07 23:15:37 x440 log: Syslog SSL connection (192.0.2.0:6514) is lost. See also FTA_SSL.3 and FTA_SSL.4.
FTP_ITC.1	TLS client session failure	See FCS_TLSC_EXT.1.
FTP_TRP.1/Admin	SSH session establishment	<182> 2022-03-10 20:04:18 x440 AAA: Login passed for user admin through ssh (192.0.2.0).
FTP_TRP.1/Admin	SSH session termination	<182> 2022-03-10 20:04:14 x440 AAA: Administrative account (admin) logout from ssh (192.0.2.0).
FTP_TRP.1/Admin	SSH session failure	See FCS_SSHS_EXT.1.

Add a DNS Name Server

The DNS client can resolve host names to IPv4 and IPv6 addresses.

About This Task

Use this procedure to specify up to eight DNS servers for use by the DNS client.

Tip

You can use the **nslookup** utility to return the IP address of a host name.

Procedure

Add a DNS name server.

```
# configure dns-client add name-server <ip-addr> vr <virtual-router-name>
```

Configure Password Settings

A password can be any combination of upper and lower case letters, numbers, and the following special characters: !, @, #, $, %, ^, *, “”, and &.

About This Task

You can configure password attributes to include the minimum length, the number of retries, and the length of time an account is locked after the maximum number of log-in failures occurs.

A user attempting to log in is prompted to enter a user name and password after establishing a successful connection. EXOS then compares the credentials against the known user database. If the credentials match, EXOS then attributes (binds) the administratively assigned role and the user is granted access.

Passwords are stored in the device in encrypted format and are obscured by asterisks.

Procedure

1. Specify that a password contain an upper-case letter, a lower-case letter, a digit, and a symbol.

   ```
   # configure account all password-policy char-validation all-char-groups
   ```

2. Specify the minimum number of characters for the password for all accounts.

   ```
   # configure account all password-policy min-length <number of characters>
   ```

   Although valid values range from 1 to 32, in an evaluated configuration the minimum password length is 15 characters.

3. Specify the maximum age, in days, for a password before a user must change their password.

   ```
   # configure account all password-policy max-age <number of days>
   ```

   Valid values range from 1 to 365.

4. Specify the number of previous passwords that the system verifies for each account.

   ```
   #configure account password-policy history 10
   ```

   In this example, users are prevented from reusing their previous 10 passwords.

5. Enable an account to be locked after a user has three consecutive failed log-in attempts.

   ```
   # configure account all password-policy lockout-on-login-failures on
   ```

6. Specify the maximum number of failed log-in attempts that are allowed before a session is terminated.

   ```
   # configure cli max-failed-logins <number of logins>
   ```

   The default is three log-ins. Valid values range from 1 through 10.

7. Enable an account to be unlocked after a specific number of minutes.

   ```
   configure account all password-policy lockout-time-period 3
   ```

   In this example, an account is unlocked after 3 minutes. Acceptable values range from 1 to 60.

8. Save the configuration.

   ```
   # save configuration
   ```

Enable and Configure SSH

You must enable SSHv2 on the switch before you can connect to the switch using an external SSHv2 client.

Procedure

1. Enable SSHv2 globally.

```
# enable ssh2
```

2. (Optional) Enable SSHv2 only on VR-Mgmt.

```
# enable ssh2 vr VR-Mgmt
```

3. Complete the following configuration tasks.
   - Generate SSH Host Keys on page 43
   - Configure the SSH Rekeying Interval on page 43
   - Enable SSH and Console Session Timeout on page 44
   - Restrict SSH Algorithms and Keys on page 45

Generate SSH Host Keys

Secure Shell 2 (SSH2) host keys are used to authenticate connections between the device and clients on remote systems.

About This Task

A host key must be generated before the device can accept incoming SSH connections. Perform this procedure from the console.

Procedure

Generate a host key.

```
# configure ssh2 key
```

Log messages indicate when the key is generated. Generation of a new key overwrites the previous key.

Configure the SSH Rekeying Interval

SSH servers rekey an SSH connection after the configured interval is reached or the configured amount of data is transferred (whichever occurs first).

About This Task

Data transmission between server and client in each SSH2 session is encrypted using session keys. Session keys are generated after negotiation between server and client using the Diffie-Hellman algorithm. Cryptanalysis experts advise that it is unsafe to use the same session key to encrypt data over long periods of time. With enough captured data, you could analyze the traffic and compromise the key, so it is advisable to keep changing the session keys after a certain interval.

You can configure the SSHv2 session rekeying interval by specifying a time interval, a data limit, or both. After the configured time interval, the SSH server forces the client to perform a key negotiation for a new session key. This new key is used for SSH communication until the next rekeying.

Procedure

1. To change the amount of data (in MB) that triggers a rekey, run the following command.

```
# configure ssh2 rekey data-limit <data-size-in-MB>
```

Note
The data limit must not exceed 1000 MB (1 GB).

2. To change the number of minutes that triggers a rekey, run the following command.

```
# configure ssh2 rekey time-interval <minutes>
```

Note
The time interval must not exceed 60 minutes. However, because the actual session can last a few seconds longer than the configured session length, set the interval to no more than 59 minutes.

After the rekeying interval is configured, the configured SSH idle timeout is disabled. Therefore, idle timeout occurs at the interval configured for console timeout. For more information, see Enable SSH and Console Session Timeout on page 44.

3. Verify the configuration.

```
# show ssh2
```

Enable SSH and Console Session Timeout

You can disconnect SSH and console sessions after they have been idle for a specified number of minutes.

About This Task

The **`configure cli idle-timeout`** command sets the timeout value for SSH and console sessions. The **`configure ssh2 idletimeout`** command disconnects idle SSH sessions at a different rate. SSH sessions are disconnected based on the lower setting.

Procedure

1. Set SSH and console sessions to be disconnected after a specified number of minutes.

```
# configure cli idle-timeout <minutes>
```

Valid values range from 1 to 240. The default is 20 minutes.

2. Set SSH sessions to be disconnected after a specified number of minutes.

```
# configure ssh2 idletimeout <minutes>
```

Valid values range from 1 to 240. 'None' is also acceptable.

3. Verify the timeout configuration.

```
# show management

CLI idle timeout    : Enabled (15 minutes)
*****
SSH2 idle timeout      : 10 minutes
```

Restrict SSH Algorithms and Keys

The claimed or allowed SSH ciphers and keys are supported only when the switch is configured in FIPS mode and when the following restrictions are configured.

About This Task

For more information, see Supported SSH Ciphers and Keys on page 18.

Procedure

1. Turn off secure mode so that only compliance algorithms are enabled.

```
# configure ssh2 secure-mode off
```

Important
If secure mode is off by default, leave it that way. Do not turn it on. Secure mode cannot be used in the evaluated configuration.

2. Set the minimum supported Diffie-Hellman group to 14, which supports group 14, 16, and 18.

```
# configure ssh2 dh-group minimum 14
```

3. Disable the following ciphers.

```
# configure ssh2 disable cipher 3des-cbc
# configure ssh2 disable cipher aes192-ctr
# configure ssh2 disable cipher aes192-cbc
# configure ssh2 disable cipher rijndael-cbc@lysator.liu.se
```

4. Disable the following public key algorithms.

```
# configure ssh2 disable pk-alg x509v3-rsa2048-sha256
# configure ssh2 disable pk-alg x509v3-ssh-rsa
```

User Key-Based Authentication

Public key authentication is an alternative method to password authentication that SSH uses to verify identity.

You can generate a key pair consisting of a private key and a public key. The public key is used by the ExtremeXOS SSH server to authenticate the user. The user public keys are stored in the switch's configuration file. These keys are then associated (or bound) to a user.

You can configure the keys on the switch in one of two ways:

- By copying the keys to the switch using SCP2 or SFTP2 with the switch acting as the server.
- By configuring the keys using the CLI. For more information, see Configure User Keys on page 46.

RSA and DSA encryption keys are supported.

SCP2 or SFTP2

The administrator can use the SCP2 or SFTP2 client software to connect to and copy the key file to the switch. The public key file must have the extension ssh. For example, `id_dsa_2048.ssh`. When the .ssh file is copied to the switch, the key is loaded into the memory. The loaded public keys are saved to the configuration file (*.cfg) when the **save** command is issued from the CLI.

The key name is derived from the file name. For example, the key name for the file `id_dsa_2048.ssh` is `id_dsa_2048`. The file name of the key or the key name is restricted to 32 characters in length.

You can associate the key with a user either implicitly, by pre-pending the user name to the file, or explicitly, using the CLI.

A key can be bound or associated only to a user that is known. In other words, that user must have an entry in the local database on the switch. After the user is authenticated, the user's rights (read-only or read/write) are obtained from the database.

The key can be associated with a user by pre-pending the user name to the file name. For example, `admin.id_dsa_2048.ssh`.

If the user specified in the file name does not exist on the switch, or if the user name is not pre-pended to the file name, the key is accepted but is not associated with a user. You can use the CLI to associate the key with the user.

Configure User Keys

You can use the command-line interface (CLI) to associate a key with a user and perform other key-related tasks.

About This Task

For details about using these commands, see the ExtremeXOS Command Reference Guide.

For more information about key files, see User Key-Based Authentication on page 45.

Procedure

1. To associate a key with a user, run the following command.

   ```
   # configure sshd2 user-key <key-name> add user <user-name>
   ```

2. To enter or paste a pregenerated host key, run the following command.

   ```
   # configure ssh2 key pregenerated
   ```

3. To write the host and user public keys to a file in the `config` directory, run the following command.

   ```
   # create sshd2 key-file {host-key|user-key} <key-name>
   ```

   The key files are created with the .ssh extension. An administrator can use this command to copy public key files to an external server.

4. To disassociate a key from a user, run the following command.

   ```
   # configure sshd2 user-key <key-name> delete user <user-name>
   ```

5. To remove a key from the database and from any associated user, run the following command.

   ```
   # delete sshd2 user-key <key-name>
   ```

Zeroization

Keys and other cryptographic items are zeroized (erased or overwritten) when various actions occur.

In some of the following scenarios, zeroization occurs when you run the **`unconfigure switch all`** command. This command resets the platform and configuration details to factory defaults.

SSH server private key

Stored in NVRAM, RAM (plain text), and FLASH. Zeroization occurs as follows when the **`unconfigure switch [all|erase]`** command is run.

- The key in NVRAM is overwritten with zeroes.
- The key in RAM overwritten by `memset` with 0.
- Keys are temporarily stored in FLASH. After a key is loaded into RAM, the key in FLASH is erased.

SSH server public key

Stored in RAM (plain text). Zeroization occurs when the **`unconfigure switch [all|erase]`** command is run. Keys are temporarily stored in FLASH. After a key is loaded into RAM, the key in FLASH is erased.

SSH session keys

Stored in RAM (plain text). Keys are cleared with 0x00 when sessions are ended.

Diffie-Hellman shared secret

Stored in RAM (plain text). The secret is overwritten with zeroes after being used by the consuming application.

Diffie-Hellman private and public parameters

Stored in RAM (plain text). The parameters are overwritten with zeroes when the key exchange is complete.

TLS client key

Stored in NVRAM. Zeroization occurs when the **`unconfigure switch erase`** command is run.

Administrative passwords

Stored in FLASH (cipher text). Zeroization occurs in the following instances.

- Encrypted passwords exist locally in a startup configuration file and are replaced with that file is edited and saved. Passwords in the file are stored in protected form only.
- Zeroization occurs when the **`unconfigure switch erase`** command is run.

PRNG seed key

Stored in RAM (plain text). Zeroization occurs when the device is turned off or restarted.

X.509 Certificate-Based Authentication

Secure syslog uses X.509 certificates for confidentiality and integrity.

The configuration in this section is assumed to be for one organization that has one root Certificate Authority (CA) and one or more issuing CAs.

Peer Configuration

The network peers in the operating environment to which EXOS will connect (using TLS) must be configured to present a valid X.509v3 identity certificate issued by a trusted CA.

Certificate Validation

Secure syslog supports server-side and client-side (mutual) authentication. When an X.509v3 certificate is presented for authentication during a TLS handshake, EXOS validates the certificate, checks the chain of trust against its internal trusted store, and performs a certificate revocation check.

Certificate validation includes the following:

- Validating the path, including checking CA certificates.
- Processing the certificate, including validation of the `extendedKeyUsage` field.
- Processing extensions, including the `BasicConstraints` extension.

Chain of trust verification includes the following:

- Validating each certificate in the chain.
- Verifying that the certificate path consists of trusted CA certificates.
- Performing revocation checks on all certificates in the path.

Important
If the connection for certificate validation cannot be established, EXOS will not accept the certificate.

TLS Negotiation

EXOS supports reference identifier matching, according to RFC 6125. The reference identifier is specified during configuration of the TLS connection. Supported reference identifiers are DNS names for the Subject Alternative Name (SAN) and the Common Name (CN).

As part of negotiating the TLS connection, EXOS verifies that the peer certificate's SAN or CN contains the expected reference identifier. The CN is checked only if the SAN is absent. Then, a connection is established only if the peer certificate is valid, trusted, has a matching reference identifier, and passes the revocation check.

Important

- If the TLS session fails because the OCSP server cannot be contacted, the administrator is instructed to verify the network path to the OCSP server and the status of the server, and to fix any issues.
- If a successful TLS session is inadvertently broken, you can reestablish the session as described in Reconnect a TLS Session on page 51.

OCSP Functionality

The revocation check uses the Online Certificate Status Protocol (OCSP) and requires a peer certificate to have its `Authority_Information_Access` extension set to an OCSP URI address.

Because the device does not perform a revocation check for the OCSP certificate, the OCSP responder (server) certificate must be signed by a trusted CA and contain the `id_pkix_ocsp_nocheck` extension.

Generate a Certificate Signing Request

The Certificate Signing Request (CSR) generates a private-key and a CSR that can be signed by a Certificate Authority (CA).

Before You Begin

Ensure that a Certificate Authority (CA) is configured.

About This Task

You use the **`configure ssl csr`** command for this task. For details about using the command, see the ExtremeXOS Command Reference Guide.

Procedure

1. Submit the CSR.

```
# configure ssl csr privkeylen <length> country <code>
organization <org-name> common-name <name>
```

2. When prompted, provide the following information for the Distinguished Name (DN), which is incorporated into the CSR.

   State or province name
   Locality name, such as a city
   Organization unit name
   Email address

   The CSR and key pair are generated. The following is an example.

```
# configure ssl csr privkeylen 2048 country US organization EXTR
common-name test
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.
For some fields there will be a default value in [].
If you enter '.' the field will be left blank.
-----
State or Province Name (full name) []: North Carolina
Locality Name (eg, city) [Default City]: Raleigh
Organizational Unit Name (eg, section) []: RDU
Email Address []: jsmith@extremenetworks.com
.................................................+++
.................+++
CSR and Key Pair generated.
-----BEGIN CERTIFICATE REQUEST-----
MIIC3TCCAcUCAQIwgZcxCzAJBgNVBAYTAlVTMQ0wCwYDVQQKDARFWFRSMREwDwYD
VQQDDAhjc3JfdGVzdDEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcM
B1JhbGVpZ2gxDDAKBgNVBAsMA1JEVTEtMCsGCSqGSIb3DQEJARYebHBldHR5am9o
bkBleHRyZW1lbmV0d29ya3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAm43c60n1XXkk1MMvK+ovX8fAhWRu8j7TAKGrSENqEhmS0BI05bjZLsj/
1oulgsPXQAl7W401OOMt5w9zcMCNmSf47PJwpQZpo4msAW8uSp7IMM9Ctv0a8oLr
kArzh3F+Gp0cAe7LycOthiXINKKWmzWpNwHmGbrwAhbd3grShurvUU7n0b+lXcle
YH5J/HnGq+j6Lb+iNF2RbCactChF0aeT7DKXZaIt8s+p9ib3XQXUNvGoP+4M/Eoq
dHfOwpvBJeL3EyhjkEmz456nwdtsY8deNi/ssW+VJJWpGPONNLo+l1wD7BksCPtJ
Pf20atDCFj6bFAo6N9gbdkh1dI3euwIDAQABoAAwDQYJKoZIhvcNAQENBQADggEB
AIkoEBWhrPmL4tf0KSgKeadfODJ6Nipkcyof9YZ9AceJhtgMmBFmMfcUrE+3e28j
asXQpEc5hLkc8fyRMNjDHuuz2d6uWju+K/TqVNTo94bvbvySFsdBKjLcOADlRP0m
CIMCCiAiaFhtmLE5Sg6BoYctJ2jRNJ4UQOejeclcG80+qaXu6u7xAg5emGMtJizE
bvePhgSdhYTCFGnqFrg3pZXHHTvRB7t54oYGG7yYdFb3jyW8CzckxnkiTV87fxHP
ojUeAwXet1AfI8coflDfmf6gKnBLMzzr5DMDmqdJgE2HgLLZCLv+JZbjbmowLrDL
DhG3F97QQkwROTpJfmrSsaU=
-----END CERTIFICATE REQUEST-----
```

```
Warning: SSL Certificate and Key will not match now.
Please load new CA signed certificate.
New Key will be usable after restart of thttpd process.
Storing the private key. This may take some time.
```

Tip
You can use the **show ssl csr** command to see the certificate request.

3. Use the following OpenSSL command to sign the CSR.

```
# openssl ca -config <config-filename> -in <CSR-filename>
-out <output-file> -extensions <cert-extension>
```

The following example uses a configuration file titled `openssl.intCA1.cnf`, a CSR titled `cert.csr.pem` in the `csr/` folder, an output file titled `cert.pem` in the `certs/` folder, and a certificate extension titled `toe-a`.

```
# openssl ca -config openssl.intCA1.cnf -in csr/cert.csr.pem
-out certs/cert.pem -extensions toe-a
```

For more information about this command, see the OpenSS Cryptography and SSL/TLS Toolkit.

Install Certificates on the Syslog Client

The secure syslog client authenticates the syslog server and encrypts messages before they are sent.

Before You Begin

Obtain the root CA certificate and the CSR-signed certificate for the syslog server.

About This Task

Secure syslog supports server-side and client-side (mutual) authentication. The EXOS syslog client performs server certificate authentication. The CSR-signed certificate is the syslog client certificate used for mutual authentication when the server requests it.

Procedure

1. Install the root certificate.

```
# download ssl <ip-addr> certificate trusted-ca <rootCA>.cert.pem
```

2. Install the CSR-signed certificate.

```
# download ssl <ip-addr> certificate csr-cert <cert>.pem ocsp on
```

3. Verify the certificates in the trusted store.

```
# show ssl trusted-ca all
```

4. (Optional) Remove a trusted CA from the trusted store.

```
# unconfigure ssl certificate trusted-ca <cert>.pem
```

5. (Optional) Remove a CSR-signed certificate.

```
# unconfigure ssl certificate csr-cert <cert>.pem
```

Reconnect a TLS Session

You can manually reconnect a TLS session that is inadvertently disconnected but not automatically reestablished.

About This Task

The system automatically attempts to reconnect a TLS session. However, if those attempts fail, for reasons such as exceeding the threshold for reconnection attempts, you can manually reconnect the session. Take the following steps to disable and then enable the syslog server in the switch, which causes the TLS session to reconnect.

Procedure

1. Disable the syslog server.

```
# disable syslog
```

2. Enable the syslog server.

```
# enable syslog
```

Configure the Banner Message

The banner messages provide information to users who access the EXOS command-line interface.

About This Task

Take the following steps to configure the message that users see before they log in and after they log in.

Procedure

1. Configure the pre-login message.

```
# configure banner before-login <message-text> save-to-configuration
```

After you press Enter (or Return), your message is applied and the text is displayed.

2. Configure the post-login message.

```
# configure banner after-login <message-text> save-to-configuration
```

After you press Enter (or Return), your message is applied and the text is displayed.

Configure IP Security Features

Configure several global IPv4 and IPv6 features.

Procedure

1. Configure several ICMP features.

```
# disable icmp redirects
# disable icmp ivp6 ignore-multicast
# disable icmp ipv6 ignore-anycast
# enable ip-security anomaly-protection icmp
```

2. Configure gratuitous ARP protection.

```
# enable ip-security arp gratuitous-protection
```

3. Disable the source route.

```
# disable ip option loose-source-route
# disable ip option strict-source-route
```

4. Set a limit on hops for router advertisements.

```
# configure ipv6 hop-limit <greater-than-32>
```

5. Enable DHCP snooping.

```
# enable ip-security dhcp-snooping [dynamic | vlan <vlan_name>]
```

6. Enable Denial of Service protection.

```
# enable dos-protect
```

Disable Unused Services

Disable any service that is not used.

Procedure

1. Disable Telnetd.

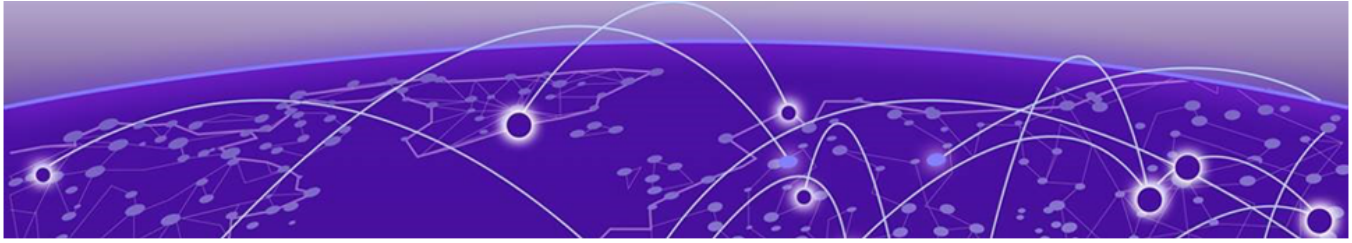
```
# disable telnetd
```

2. Disable web access.

```
# disable web http
# disable web https
```

3. Disable the iqagent application.

```
# disable iqagent
```



Network Time Protocol

Network Time Protocol (NTP) synchronizes the time on devices across a network that has variable latency (time delay).

Overview

NTP provides a coordinated Universal Time Clock (UTC), the primary time standard by which the world regulates clocks and time. UTC is used by devices that rely on having a highly accurate, universally accepted time, and can synchronize computer clock times to a fraction of a millisecond.

NTP uses a hierarchical, semi-layered system of levels of clock sources called a stratum. Each stratum is assigned a layer number starting with 0 (zero), with 0 meaning the least amount of delay. The layer number defines the distance, or number of NTP hops away, from the reference clock. The lower the number, the closer the device is to the reference clock.

ExtremeXOS version 31.3.100 uses NTPv3.

SNTP is a simplified version of NTP that uses the same protocol, but without many of the complex synchronization algorithms used by NTP. SNTP is suited for use in smaller, less complex networks. For more information, see Using the Simple Network Management Protocol in the *ExtremeXOS User Guide*.

Note
As a best practice, do not update the time manually when NTP is enabled.

Limitations

The Extreme Networks implementation of NTPv3 has the following limitations.

- SNTP cannot be enabled while NTP is enabled.
- The NTP multicast delivery mechanism is not supported.
- The NTP autokey security mechanism is not supported.
- The broadcast client option cannot be enabled per VLAN.

- NTP authentication can be enabled globally and, optionally, per virtual router (VR).
- Virtual routing and forwarding (VRF) is not supported.

Add or Delete the NTP Server

You can add or delete the NTP server and then verify that the action was successful.

Procedure

1. Add the NTP server.

   ```
   # configure ntp server add <ip-addr> key <key-id> vr VR-Mgmt
   ```

   Valid values for the key ID range from 1 to 65534. If you do not specify a name for the VR, the current command context is used.
2. Delete the NTP server.

   ```
   # configure ntp server delete <ip addr>
   ```
3. Verify that the server was added or deleted.

   ```
   # show ntp server
   ```

Configure NTP Over Virtual Routers

You can configure NTP over multiple virtual routers (VR).

About This Task

The following steps show you how to enable NTP on a VR, over a VLAN, and in all VLANs for a VR.

Procedure

1. Enable NTP on a specified VR.

   ```
   # enable ntp vr <vr-name>
   ```

   If you do not specify a VR name, NTP is enabled in the VR of the current command context.
2. Enable NTP over a specified VLAN.

   ```
   # enable ntp vlan <vlan-name>
   ```
3. Enable NTP over all VLANs for a specified VR.

   ```
   # enable ntp all vr <vr-name>
   ```

Manage NTP Authentication

To prevent false time information from unauthorized servers, enable NTP to allow an authenticated server and client to exchange time information.

About This Task

Two authentication methods are supported: the MD5 Message-Digest Algorithm and SHA-256. However, when FIPS mode is enabled, NTP uses the OpenSSL FIPS library and supports only SHA-256, which is a FIPS-compliant algorithm for authentication. When FIPS mode is enabled, MD5 key configuration support is not available and existing MD5 key configurations are removed. For more information, see the Federal Information Processing Standards (FIPS) Mode section of the *ExtremeXOS User Guide*.

At a high level, the process for managing NTP authentication is as follows.

- First, enable NTP authentication globally on the device.
- Then, create an NTP authentication key, configured as trusted, to check the encryption key against the key on the receiving device before an NTP packet is sent.
- At this point, an NTP server, peer, and broadcast server can use the NTP authenticated service.

Procedure

1. Enable NTP authentication globally on the device.

```
# enable ntp authentication
```

2. Create a SHA-256 key.

```
# create ntp key <keyid> sha256
(Press Enter or Return)
Key: <key-string>
```

3. Configure the key as trusted.

```
# configure ntp key <keyid> trusted
```

Configure NTP Restrict Lists

You use a restrict list to deny or permit the NTP service for a specified host or network.

About This Task

When an NTP server is configured, the server IP address is automatically added to the restrict list with a permit action. When NTP is enabled over a VLAN, the IP addresses in the VLAN are automatically added to the restrict list with a permit action.

The following are a few configuration examples. For more information, see the configure ntp retstrict-list command in the *ExtremeXOS Command Reference Guide*.

Procedure

1. Deny the NTP service to a specified IP address in the current command context.

```
# configure ntp restrict-list add <network/mask> deny
```

2. Deny the NTP service to a specified IP address in a specified VR.

```
# configure ntp restrict-list add <network/mask> deny vr <vr-name>
```

3. Permit the NTP service to a specified IP address in the current command context.

```
# configure ntp restrict-list add <network/mask> permit
```

4. Permit the NTP service to a specified IP address in a specified VR.

```
# configure ntp restrict-list add <network/mask> permit vr <vr-name>
```

Disable the NTP Broadcast Client

Disable the NTP broadcast client, which listens for NTP packets from an NTP broadcast server.

About This Task

This functionality is global and cannot be configured per VLAN.

Procedure

1. Disable the broadcast client in the current command context.

```
# disable ntp broadcast-client
```

2. Disable the broadcast client in the specified VR.

```
# disable ntp broadcast-client vr <vr-name>
```

Display NTP Information

You can use various **show** commands to display information such as the global NTP status and NTP key information.

About This Task

The following examples show typical output for the commands. Your output will vary. For more information about command options, see the ExtremeXOS Command Reference Guide.

Procedure

1. Display the global NTP status of the device.

```
# show ntp
NTP                 : Enabled
Authentication      : Disabled
Broadcast-Client    : Disabled
VR                  : VR-Default
```

2. Display the system status based on the most reliable clock server or NTP server.

```
# show ntp sys-info
System Peer          : 0.us.pool.ntp.org
System Peer Mode     : Client
Leap Indicator       : 00
Stratum              : 3
Precision            : -20
Root Distance        : 0.09084 second
Root Dispersion      : 0.23717 second
Reference ID         : [216.93.242.12]
Reference time       : d140571d.e8389ff7  Fri, Apr  1 2011  6:52:29.907
System Flags         : Monitor, Ntp, Kernel, Stats, Authentication
Jitter               : 0.004700 second
Stability            : 0.000 ppm
Broadcast Delay      : 0.007996 second
Auth Delay           : 0.000000 second
```

When NTP authentication is enabled, "Authentication" is listed in the System Flags section of the output.

3. Display NTP VLAN configurations for a specified VR.

```
# show ntp vlan vr VR-Default
VR Name          Vlan            NTP Status  Broadcast Server  Key Index
================================================================================
VR-Default       Default         Disabled    Disabled          -
VR-Default       vlan1           Disabled    Disabled          -
```

4. Display NTP configurations for a specified VR.

```
# show ntp vr vr1
NTP                 : Enabled
Authentication      : Disabled
Broadcast-Client    : Disabled
VR                  : vr1
```

5. Display NTP clock source information, such as delay and offset, for the VR of the current command context.

```
# show ntp association

VR Name     Remote          Reference ID    St Poll Reach Delay   Offset   Disp
=========== =============== =============== == ==== ===== ======= ======== =======
VR-Mgmt      !45.125.255.53 223.255.185.2   2  64   1     0.01172 -0.08789 1.98431
VR-Mgmt      !10.127.2.255  BCST            16 64   0     0.00000 +0.00000 4.00000
```

6. Display NTP key information.

```
# show ntp key
Key Index        Trusted    Auth      Key String (encrypted)
=================================================================
200              Yes        SHA-256   23:24:6c:35:4a:35:79:74:65
```

7. Display NTP restrict list information for a specified VR.

```
# show ntp restrict-list user vr "VR-Mgmt"
VR Name          IP Address      Mask                Count Type   Action
=============================================================================
VR-Mgmt          1.1.1.1         255.255.255.255         0 User   Permit
```