Extreme NetIron Configuration Guide for Common Criteria NDcPP 2.1

06.3.00aa

9037138-00 Rev AA
July 2021

Legal Notice

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

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

Trademarks

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

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

For additional information on Extreme Networks trademarks, 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/

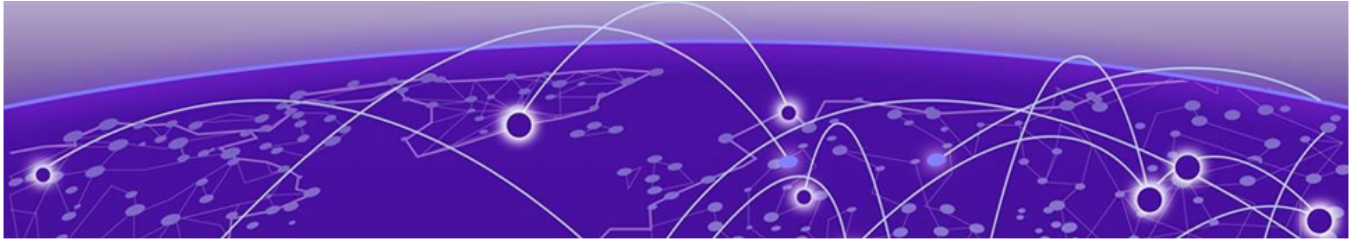


Table of Contents

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.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	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, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*`[`*member*`...]`.
\	In command examples, the backslash indicates a “soft” line break. When 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:

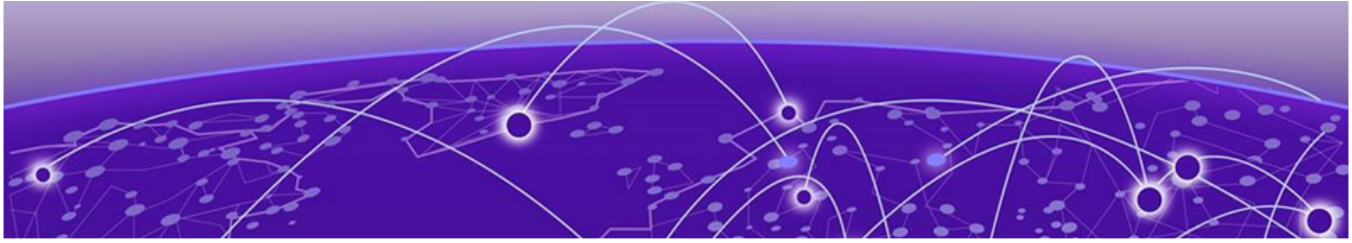
- Content errors, or confusing or conflicting information.

- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

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

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

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



About This Document

Supported hardware and software

The following hardware platforms are supported by FIPS and Common Criteria:

- Extreme NetIron CER 2000-4X-RT Series
- Extreme NetIron MLXe Series with BR-MLX-MR2-X management card

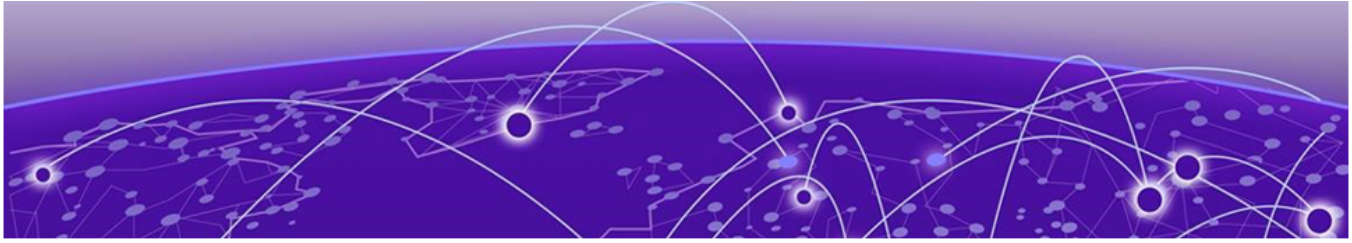
To determine if the Extreme device and current software version is Common Criteria certified, refer to https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm.

What's new in this document

For the complete list of supported features and the summary of enhancements and configuration notes for this release, refer to the NetIron 6.3.00a Release Notes.

The new features for this release are:

- OpenSSL upgrade to version 1.0.2p with FIPS Module version 2.0.16 for both Extreme NetIron CER and MLXe series platforms
- SSH rekey based on volume of traffic(1GB)
- SSH rekey based on Timer
- RFC 6960- OCSP support for certification Revocation with TLS over Syslog, Radius, TACACS+ and HTTPs copy
- RFC 5280- TLS client authenticating the server X.509v3 digital certificate
- Audit logs for SSH, OCSP and TLS



Common Criteria Certification

Common Criteria overview

This section contains steps for configuring the Extreme NetIron for Common Criteria (CC) standards with OS version 06.3.00aa collaborative Protection Profile for Network Devices (NDcPP) version 2.1.

Common Criteria certification for a device enforces a set of security standards and feature limitations on a device to be compliant with the Common Criteria standards, similar to placing the device in FIPS mode. To better understand the Common Criteria certification and the associated security functions that have been subject to certification, refer to the document *Extreme NetIron R06.3.00aa (NDcPP21) Security Target*.

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

Extreme NetIron switches running OS 06.3.00aa are designed to support FIPS-compliance mode. All cryptographic algorithms required and used in CC are certified by the Cryptographic Algorithm Validation System (CAVS). The RNG component does not require configuration and follows the specified requirements as above.

The Extreme NetIron management functions are isolated through user authentication. After completing successful login, all actions are audited. In addition, the remote management communication path is protected against modification and disclosure using SSHv2. The audit channel to an external Syslog server is protected using TLS encapsulation for NDcPP evaluation. The authentication channel between the TOE and external authentication servers like RADIUS or TACACS+ must be configured to be protected using TLS encapsulation.

Note
Common Criteria mode becomes available once a device is FIPS-enabled.

Note
To determine if the NetIron device and current software version is Common Criteria-certified, refer to https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm. Refer to the release notes for the software version running on the device to verify that the software is FIPS-and Common Criteria-certified.

You can enable Common Criteria mode on a device directly from non-FIPS mode, or on a device already in FIPS mode. The following table summarizes the transitions.

Table 4: Transition to Common Criteria mode

From	To non-FIPS mode	To FIPS mode	To Common Criteria mode
Non-FIPS mode	Not applicable	Use the **`fips enable`** command	Use the **`fips enable common-criteria`** command
FIPS mode	Use the **`no fips enable`** command	Not applicable	Use the **`fips enable common-criteria`** command
Common Criteria mode	Use the **`no fips enable`** or **`no fips enable common-criteria`** command	Use the following commands in a sequence: 1. **`no fips enable`** 2. **`reload device`** 3. **`fips enable`**	Not applicable

Following considerations are advised:

- Disabling FIPS mode from the Common Criteria mode using the **`no fips enable`** command downgrades the device directly into the non-FIPS mode.
- You cannot directly transition from Common Criteria mode to FIPS mode. To transition to FIPS mode, you must disable FIPS mode, reload the device, and then enable FIPS mode.

The following table lists the individual Extreme NetIron platforms that support Common Criteria certification requirements.

Table 5: Devices that support Common Criteria

Features supported	Extreme MLX Series	Extreme NetIron CER 2000-4X-RT Series
FIPS CC mode	MLXe: Yes MLX: No	Yes

Establishing a serial connection

About This Task

Caution

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

About This Task

Follow the steps given below to attach a management station using the serial port.

Procedure

1. Connect a PC or terminal to the serial port of the system using a straight-through cable. The serial port has a male DB-9 connector.

   Note

   You need to run a terminal emulation program on the PC.

2. Open the terminal emulation program and set the session parameters as follows:
   - Baud: 9600 bps
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None

   When you establish the serial connection to the system, press Enter to display the CLI prompt in the terminal emulation window. For example:

   ```
   device>
   ```

   If you see this of these prompt, you are now connected to the system.

   You can customize the prompt by changing the system name. For more information, refer to the *Extreme NetIron Management Configuration Guide*.

   If you do not see one of these prompts, follow the instructions given below.
3. Make sure the cable is securely connected to your PC and to the system.

4. Check the settings in your terminal emulation program. In addition to the session settings listed above, make sure the terminal emulation session is running on the same serial port you attached to the system.

   The EIA/TIA 232 serial communication port serves as a connection point for management by a PC or SNMP workstation.

Setting the Management IP address of the Device

About This Task

For system management, you must assign an IP address on the active management port. If the active management module becomes unavailable and the redundant module becomes the active module, the IP address is automatically assigned to the new active management module.

For example, to assign the IP address 10.0.1.1 to the management module, use these steps.

Procedure

1. At the opening CLI prompt, enter **enable** .

```
device# enable
```

2. Enter the **erase startup-config** command at the Privileged EXEC level prompt (for example, device#), then press **Enter**. This command erases the factory test configuration if it is still present.

```
device# erase startup-config
```

   After entering this command, perform a reload on the system.

   Caution
   Use the **erase startup-config** command only for new systems. If you enter this command on a system you have already configured, the command erases the configuration. If you accidentally do erase the configuration on a configured system, enter the **write memory** command to save the running configuration to the startup-config file.

3. Access the configuration level of the CLI by entering the **configure terminal** command.

```
device# configure terminal
device(config)#
```

4. Configure the IP address and mask for the management interface by entering these commands.

```
device(config)# interface management 1
device(config-if-mgmt-1)# ip address 10.0.1.1/24
```

5. Enable the strict password check on the device by entering this command.

```
device(config)# enable strict-password-enforcement
```

6. To enable SSH access, generate SSH host keys by using the following command

```
device(config)# crypto key generate
```

7. To configure the authentication for the SSH user, use the following command.

```
device(config)# aaa authentication login default method-list
device(config)# aaa authentication login privilege-mode
```

8. To configure the valid user credentials either local on the device or on the remote authentication server, use the following command.

```
device(config)# username id password
(Enter new password:)********
```

Device Access

Once an IP address is assigned to the Extreme Networks device's management port, you can access the CLI through a network connection using SSH on its 10BaseT/100BaseTX Ethernet (management) port. This is in addition to the console port connection over the device's serial port.

You can initiate a SSH connection by specifying the management port's IP address.

The commands in the CLI are organized into the following levels:

- User EXEC - Lets you display information and perform basic tasks such as pings and traceroutes.
- Privileged EXEC - Lets you use the same commands as those at the User EXEC level plus configuration commands that do not require saving the changes to the system-config file.
- CONFIG - Lets you make configuration changes to the device. To save the changes across software reloads and system resets, you need to save them to the system-config file. The CONFIG level contains sub-levels for individual ports, for VLANs, for routing protocols, and other configuration areas.

Note

By default, any user who can open with command line interface (CLI) connection to an Extreme Network device can access all these CLI levels. To secure access, you can configure Enable passwords or local user accounts, or you can configure the device to use a RADIUS or TACACS+ server for authentication.

To access the device using SSH from a remote client:

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

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

The configured max-retry value is optional and must be set between 1 and 5 per the security target. If the administrator provides the incorrect credentials after the specified number of retries, the account will lock up based on the login-attempts configured. For example, if the login-attempt is configured as 2, then account lock-up will happen at 3 incorrect attempts. There is no maximum lockout duration.

```
device(config)#username abcd…. ?
  access-time                   access permission based on time of the day
  enable                        Enable the user for login access after disabled
  expires                       Password expire time in days (1-365)
  login-attempts                Set number of login attempts
  nopassword                    No password is required for the user to log in
  password                      Specify the password for the user
  privilege                     Set user privilege level
```

```
device(config)#username abcd login-attempts ?
  DECIMAL   Range <1 to 5>
```

Locked user can access through the console and respective locked account will be unlocked on successful logging. All other locked accounts remain locked. All locked accounts will be unlocked when the device is reloaded. A locked account can be unlocked by using the command:

```
device# username <user> enable
```

Console(local) and remote network connections can be terminated by issuing “exit” from the command prompt until the prompt requesting user authentication is shown.

Password Requirements

The TOE enforces minimum password length and allows passwords from a set of upper-case, lower-case, numeral and special characters.

In addition to the these settings, additional OPTIONAL restrictions can be imposed by calling the command **enable strict-password-enforcement**.

```
device(config)# enable strict-password-enforcement
```

If **enable strict-password-enforcement** is executed and a user logs in and attempts to change their own user password, the following prompt is displayed:

```
Enter old password
```

After validating the old password, the following prompt is displayed:

```
Enter new password
```

These are the additional restrictions when strict-password-enforcement is in force:

The minimum password must be at least eight (8) and up to forty eight (48) characters to be CC compliant. The TOE requires that password should have:

- Must consist of characters from three or more chararacter classes, uppercase, lowercase, numeric, special characters (!, @, #, $, %, ^, &, *, (, and) are valid.).
- Must not begin with the only uppercase character in the password. (Strict password enforcement only)
- Must not end with the only numeric character in the password. (Strict password enforcement only)

The administrator can set the minimum password length with the following command and ensure that this length must be at least eight and a maximum of forty eight:

```
device# enable password-min-length <length>
```

Features unavailable in Common Criteria mode

Some of the security features that are allowed in FIPS mode are disabled in Common Criteria mode: Though following three features are also not allowed in FIPS either.

- SSHv2: Host and client key generation methods using DSA and the RSA-1024 key size are not supported (only RSA 2048 and higher key sizes are supported). Therefore, the following commands are not supported:
  - **crypto key generation dsa**
  - **crypto key client generation dsa**
  - **crypto key zero dsa**
  - **crypto key client zero dsa**
  - **crypto key gen rsa modulus 1024**
  - **crypto key zero rsa modulus 1024**
- TLS and HTTPS: The RSA 1024 key size for SSL or TLS private key generation is not supported (NetIron devices support only 2048 and above key sizes).
- SSH key exchange: The SSH key exchange method Diffie-Hellman-Group1-Sha1 is not supported. Only Diffie-Hellman-Group14-Sha1 is supported.
- Common Criteria specific Syslog: Logging to a host that uses UDP for transport is not supported. Only the TLS host is supported. Therefore, the **logging host** [**ipv4**] { *ip-address* } **udp-port** *port* command is not supported.
- Common Criteria specific: For authentication server RADIUS, UDP is not supported and for TACACS +, TCP is not supported.

Enabling Common Criteria mode

When you enable Common Criteria mode on the device, it enters the Common Criteria Administrative mode. Common Criteria mode configures the cryptographic features of the device such that only CC approved cryptography is used.

- Common Criteria Administrative mode: Log in to the device console and enable the Common Criteria mode. You can optionally modify the default Common Criteria security policy in this mode.

  Note
  When you use the **reload** command to reload the device, the validation of software image with the signature file is triggered. Failure in signature verification results in the device continuously rebooting after device reload.

- Common Criteria Operational mode: Transition to Common Criteria operational mode from Common Criteria Administrative mode. After you transition the device to the Operational mode, you must save the configuration and reboot the device.

Note
When the NetIron device is in FIPS mode, the RSA2048-SHA256-based signature firmware integrity check is done during the image installation and during image reload.

Entering Common Criteria Administrative mode

You can enable Common Criteria mode on a device with the following command.

```
device(config)# fips enable common-criteria
```

Syntax: **[no] fips enable common-criteria**

The device prompt displays the detailed banner information shown in the following example.

```
Device(config)#fips enable common-criteria
WARNING: This will enable FIPS and Common Criteria on this device. Please refer
       : to the NetIron Federal Information Processing Standards Guide for
       : more details. Also, be advised that Software/Firmware Integrity checks
       : will always be performed on this device on subsequent reloads, even
       : if FIPS or Common Criteria is disabled in the future.
Are you sure? (enter 'y' or 'n'): y
This device is now running in CC administrative mode.
At this time you can alter this system's CC default security policy
and then enter CC operational mode.

Note: Making changes to the default CC security policy weakens
the security of the device and makes the device non-compliant
with CC and FIPS 140-2 Level 2, design assurance Level 3.
The default security policy defined in the FIPS
Security Policy Document ensures that the device complies with all
FIPS 140-2 specifications. Commands to alter the default security policy
are available to the crypto-officer; however, Extreme does not recommend
making changes to the default security policy at any time.
====================================

To enter CC mode, complete the following steps:
1. Optionally, configure FIPS policy commands that meets your network
   requirements. You must explicitly configure the following services if you
   want to use them when the device is operational in CC mode:
      - Allow TFTP access.
          Current status: Enabled
      - Allow SNMP Access to the Critical Security Parameter (CSP) MIB objects.
          Current status: Disabled
      - Allow access to all commands within the monitor mode.
          Current status: Disabled
      - Allow cleartext password display in some commands.
          Current status: Disabled
      - Retention of shared secret keys for all protocols and the host passwords.
          Current status: Retain
      - Retention of SSH RSA host keys.
          Current status: Retain

2. Enter the "fips zeroize all" command, which zeroes out the shared secrets
    used by various networking protocols, including the host access passwords,
    SSH and HTTPS host-keys with the digital signature based on the configured
    FIPS Security Policy.
3. Save the running configuration.
4. Reload the device.
5. Enter the "fips show" command to verify that the device entered
  FIPS or CC operational mode.
====================================

In FIPS mode, the system will disable the following services or commands after
reload:
FIPS. Telnet server will be disabled.
      The "telnet server" command will be removed.
FIPS. SSL Client will be enabled.
FIPS. TLS version 1.0 will be disabled.
```

```
FIPS. SCP will be enabled.
      The "ip ssh scp disable" command will be removed.

FIPS. SNMP server will change as follows:
      -SNMP support for v1 and v2c versions will be disabled.
      -For SNMPv3 version authentication and privacy is mandatory,
       and MD5 authentication key and DES privacy password will be disabled.
FIPS. NTP md5 authentication will be disabled.
FIPS. HTTP Client will be disabled.
FIPS. For SSH Key Exchange, only diffie-hellman-group-exchange-sha256
    algorithm is allowed.
FIPS. Passwords/Keys which don't comply with FIPS standards will be removed
      on reload.
FIPS. Please see FIPS config guide for complete details.

FIPS. Configuration "enable aaa console" will be disabled temporarily to
      allow console access to configure SSH parameters. It can be
      re-enabled after SSH is confirmed operational
      Current status of "enable aaa console" is: Disabled

====================================
Additionally, in CC operational mode, following are the restrictions
on system services or commands after reload:
CC. Syslog servers need to use TLS encapsulation(see exception below in VPNGW).
CC. TACACS+ servers need to use TLS encapsulation(see exception below in VPNGW).
CC. All versions of SNMP will be disabled.
CC. DSA keys will be deleted from configuration, and will be disabled.
CC. RSA key sizes will be restricted to 2048 and above in the configuration.
CC. RADIUS servers must be used over TLS (see exception below in VPNGW).
CC. For SSH Key Exchange, only diffie-hellman-group14-sha1 algorithm is allowed.

In CC VPN Gateway mode, since all traffic must be tunneled within IPSec
using the in-band ports, here are the guidelines:
VPNGW. Management port should not be used since management module does
       not have IPSec stack
VPNGW. Syslog servers could be configured to use UDP. TLS encapsulation is not
       mandatory since IPsec encapsulation is present.
VPNGW. TACACS+ servers could be configured to use TCP. TLS encapsulation is not
       mandatory since IPsec encapsulation is present.
VPNGW. RADIUS servers could be configured to use UDP. TLS encapsulation is not
       mandatory since IPsec encapsulation is present.
VPNGW. The required logging needs to be separately enabled:
       "logging enable ikev2 extended"
       "logging enable pki pki-extended"
VPNGW. The NAT-T needs to be separately enabled:
       "ikev2 nat-enable"
==================
```

Entering Common Criteria Operational mode

When the device is in Common Criteria Administrative mode, perform the following steps to place the device into Common Criteria Operational mode.

Procedure

1. Configure the local user accounts as secure and delete non-secure user accounts. A local user account is secure when it has a password with characters from three or more character classes. These character classes are uppercase, lowercase, numeric, and ASCII non-alphanumeric characters.
2. Configure secure logging by setting up the encrypted Syslog server. For details, refer to Appendix C: Configuring an external Syslog Server with TLS support.

3. Use the **enable aaa console** command to ensure user authentication during the next reload. This also requires that you have enabled AAA authentication with the **aaa authentication login default** command.
4. Use the **aaa authentication login privilege-mode** command. It allows you to login directly to privilege mode.
5. Use the **write memory** command to save the configuration.
6. Reload the device.

What to Do Next

On successful completion of these steps, the device will be in Common Criteria Operational mode.

Displaying Common Criteria information

After you have enabled Common Criteria Administrative mode on the device, you can display the information with the **fips show** command.

```
Device#fips show
FIPS Validated Cryptographic Module
MP FIPS Version: EXTR-NI-MP-CRYPTO-VER-4.0
LP FIPS Version: EXTR-NI-LP-CRYPTO-VER-2.0
LP IPsec FPGA FIPS Version: EXTR-NI-LP-FPGA-CRYPTO-VER-1.0
FIPS mode   : Administrative status ON: Operational status OFF
FIPS CC mode: Administrative status ON: Operational status OFF

System Specific:
OS monitor access status is: Disabled

Management Protocol Specific:
Telnet server                  : Disabled
Telnet client                  : Disabled
TFTP client                    : Disabled
HTTPS SSL 3.0 TLS 1.0          : Disabled
SNMP v1, v2c, v3               : Disabled
SNMP Access to security objects: Disabled
Password Display               : Disabled
Any AAA server (including      :
                TACACS, None) : Disabled
Critical security Parameter updates across FIPS boundary:
(i.e. during "fips zeroize" ..., or "no fips enable")   :
Protocol Shared secret and host passwords: Clear
SSH RSA Host keys                        : Clear
HTTPS RSA Host Keys and Signature        : Clear
```

Note
The HTTPS RSA host keys and signature are for the MLXe chassis only; not available for the NetIron CER device.

After you have enabled Common Criteria Operational mode by zeroizing the FIPS keys, saving the configuration, and reloading the device, enter the **fips show** command to verify the operational mode status.

```
device# fips show
FIPS Validated Cryptographic Module
MP FIPS Version: EXTR-NI-MP-CRYPTO-VER-4.0
LP FIPS Version: EXTR-NI-LP-CRYPTO-VER-2.0
LP IPsec FPGA FIPS Version: EXTR-NI-LP-FPGA-CRYPTO-VER-1.0
```

```
FIPS mode : Administrative status ON: Operational status ON
FIPS CC mode: Administrative status ON: Operational status ON

System Specific:
OS monitor access status is: Disabled

Management Protocol Specific:
Telnet server                  : Disabled
Telnet client                  : Disabled
TFTP client                    : Disabled
HTTPS SSL 3.0 TLS 1.0          : Disabled
SNMP v1, v2c, v3               : Disabled
SNMP Access to security objects: Disabled
Password Display               : Disabled
Any AAA server (including      :
                TACACS, None) : Disabled
Critical security Parameter updates across FIPS boundary:
(i.e. during "fips zeroize" ..., or "no fips enable")   :
Protocol Shared secret and host passwords: Clear
SSH RSA Host keys                        : Clear
HTTPS RSA Host Keys and Signature        : Clear
```

Table 6: fips show command output description

Field	Description
OS monitor access status is	The following policy allows full access to the OS monitor mode. This includes read, write access for debug purposes: **fips policy allow monitor-full-access**.
Telnet server	Telnet client and server are always disabled in FIPS CC Operational mode.
Telnet client	Telnet client and server are always disabled in FIPS CC Operational mode.
TFTP client	To allow TFTP access in FIPS mode, use **fips policy allow tftp-access**.
HTTPS SSL 3.0 TLS 1.0	Always disabled in FIPS mode.
SNMP v1, v2c, v3	Always disabled in FIPS CC mode.
SNMP	SNMP Access is disabled in FIPS CC mode.
Password Display	Disabled in FIPS CC mode.
Any AAA server	To allow any AAA server (including RADIUS and TLS support for TACACS+ servers) to be used in FIPS CC mode, use **fips policy allow common-criteria aaa-server-any**.

Table 6: fips show command output description (continued)

Field	Description
Protocol shared secret and host passwords	To retain the protocol shared secrets and host access passwords between FIPS mode and non-FIPS mode, use **fips policy retain shared-secrets**.
HTTPS DSA Host keys	To retain the SSH RSA host keys between FIPS mode and non-FIPS mode, use fips policy retain rsa-host-keys (for MLX platform only).

Note
Making changes to the default FIPS security policy weakens the security of the device and makes the device non-compliant with FIPS 140-2. The default security policy defined in the FIPS Security Policy document ensures that the device complies with all FIPS 140-2 specifications. Commands to alter the default security policy are available to the Crypto-officer; however, Extreme does not recommend making changes to the default security policy at any time.

Downloading firmware from Extreme's website

Perform the following tasks to download the firmware.

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

   Note
   File location and version details are provided to the customer.

2. Download and verify with the downloaded image with the appropriate file signature verification (md5sum or other MD5 checksum utility).

   Note
   The MD5 verification detects file transfer errors for the downloaded file and that the file is provided by Extreme Networks. However, only the embedded cryptographic signatures described in the next section provide assurance that the update is a valid firmware package from Extreme Networks.

Simplified firmware upgrade

Simplified Upgrade is a single operation that performs a full system upgrade of all the images. The routing and switching functionalities will continue to operate until TOE is reloaded after upgrade is done. It can be as simple as one command from the CLI. However using the **copy tftp system** command with the new all images and manifest parameters introduced in R05.3.00, you can upgrade your system by issuing only one command.

Use the following command to perform the simplified switch upgrade:

Enable TFTP in FIPS CC mode :

```
fips policy allow tftp-access
```

For Extreme NetIron MLX Series devices :

copy tftp system all <Ip addres for the tftp server> manifest <manifest text file name>

The firmware packages are signed using a 2048-bit RSA key with SHA-256 during firmware build and is verified during firmware installation using a public key file on the switch. The digital signature contained within the firmware package is the definitive method to determine the validity of the firmware during download and installation. The installation begins after a successful verification, and an error message displays upon unsuccessful verification.

The process is optimized by introducing a version-check of the images to determine whether it is necessary to download/upgrade the image or not. This simplified upgrade method greatly reduces the possibility of having incompatible interface modules due to incompatible image versions.

The command can be issued to download images from either of the following:

- TFTP server
- auxiliary storage device

Use the all-images parameter to upgrade the management and interface boot, monitor, and application images, as well as all interface and management FPGA images. Since many of these images are not required to be upgraded for each release and doing so can be time consuming, you can upgrade the management and interface monitor and application images, as well as the combined FPGA images only by omitting the all images parameter.

The default behavior is that the all images parameter is not specified.

Note

Management and interface boot images and individual boot images are generally not required to be upgraded and customers are not recommended to upgrade them, unless it is explicitly stated otherwise in release notes. Copying management interface FPGA images may temporarily affect time-sensitive protocols.

Note

For simplified upgrades on the NetIron CER devices, the pbif_mero installation in simplified upgrade will fail and device will need to be reloaded. After all images are installed using Simplified upgrade, the pbif will need to be installed manually, and the device will need to be reloaded again.

Note

For a simplified upgrade from R05.6.00d to R05.7.00a, b, or c, the boot image is not upgraded as part of the manifest file due to it not being a necessary upgrade. The 5.6.00 boot image is compatible with the 5.7.00 version. When a **show version** is run on the Extreme MLX device, it will show the boot image as version 5.6.00, but the Extreme MLX device will be fully functional, and have the full update of 5.7.00c. You may still choose to manually upgrade to the R05.7.00 boot image. Both use cases are acceptable and will function properly on the Extreme MLX device.

Extreme NetIron MLX Series single-command (full-system) upgrade

There is no change in the syntax for the full-system upgrade.

Syntax: `copy tftp system all-images<server-ip-address> manifest <File name> [lp-sec | mp-sec | secondary]`

Syntax: `copy <slot1 | slot2> system manifest <File name> [lp-sec | mp-sec | secondary]`

Note
Boot images are not included in the upgrade process for systems running Multi-Service IronWare Release 05.6.00d and later when the "all-images" option is used. The optional keyword "all-images" specifies to include only the MP FPGA images (MBRIDGE/MBRIDGE32 and SBRIDGE/HSBRIDGE).

Extreme NetIron CER single-command (full-system) upgrade

Note
Boot images are not included in the upgrade process for systems running Multi-Service IronWare Release 05.6.00d and later when the "all-images" option is used.

Syntax: `copy tftp system <server-ip-address> manifest <File name>`

Step 1: Download Manifest file and Validation

Note
While the simplified upgrade is in progress, CLI commands or SNMP set-requests that initiate a TFTP download are rejected.

When you issue the **`copy tftp system`** command using the manifest parameter, the first step the system performs is to download the digital signature file associated with the manifest file, download the manifest file and perform a signature check. This ensures the manifest file download is indeed created by Extreme, and not modified by others.

Step 2: Download File Images

Next, the system upgrades the system file images. The file images upgraded depend on how you enter the command. If you use the manifest and all images parameters, the files are upgraded in the following sequence:

- management module Boot image
- interface module Boot image
- management module Monitor image
- interface module Monitor image
- management module Application image
- interface module Application image
- Bundled FPGA image for all interface modules

- MBRIDGE
- SBRIDGE

If you do not use the all images parameter, the files are upgraded in the following sequence:

- management module Monitor image
- interface module Monitor image
- management module Application image
- interface module Application image
- Bundled FPGA image for all interface modules

The system takes following steps in downloading and installing the images.

Downloading the images

About This Task

It takes the following steps:

1. Perform a signature check of the manifest file.
2. Open the manifest file to lookup for the filename of the image and its relative path.
3. All images and signature files are first downloaded and saved to temporary files in the embedded Slot1 compact flash.
4. After all the images are successfully downloaded, the system will first perform a CRC check and then proceed to verify all the signatures of each binary. If there's any failure, the upgrade is aborted and a Syslog message is posted.

It will repeat the same steps for all images necessary for the upgrade.

If an image cannot be located, an error is logged and it will proceed to boot with application and monitor images synced from the MP.

Sample output of the Simplified upgrade

This is a sample output of the simplified upgrade for a Extreme NetIron MLX series device.

```
device#copy tftp system 10.20.81.154 manifest MLX06300aa_Manifest.txt
.TFTP: Download to flash done.
.TFTP: Download to flash done.
Verified OK
FIPS: Image verification passed for manifest_tmp

SYSLOG: <14>Aug  9 2019 19:40:39 FIPS: Image verification passed for manifest_tmp

SYSLOG: <14>Aug  9 2019 19:40:39 Single-command upgrade started.

1) Download MP monitor image /Monitor/ManagementModule/xmb06200.bin from tftp 10.20.81.154
................................TFTP: Download to flash done.

2) Download LP monitor image /Monitor/InterfaceModule/xmlb06200.bin from tftp 10.20.81.154
................................TFTP: Download to flash done.

3) Download MP application image /Application/ManagementModule/xmr06300aa.bin from tftp
10.20.81.154 to primary:
................................................................................
................................................................................
```

```
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
.............................TFTP: Download to flash done.

4) Download LP application image /Application/InterfaceModule/xmlp06300aa.bin from tftp
10.20.81.154 to primary:
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
.......................................TFTP: Download to flash done.

5) Bundle LP FPGA skipped, same FPGA versions exist.

1) Install MP monitor image /Monitor/ManagementModule/xmb06200.bin from tftp 10.20.81.154
..............................Verified OK
FIPS: Image verification passed for monitor

SYSLOG: <14>Aug  9 2019 19:41:31 FIPS: Image verification passed for monitor
Done

2) Install LP monitor image /Monitor/InterfaceModule/xmlb06200.bin from tftp 10.20.81.154
Save a copy to MP's flash, please wait.....................................Verified OK
FIPS: Image verification passed for lp-monitor-0

SYSLOG: <14>Aug  9 2019 19:41:34 FIPS: Image verification passed for lp-monitor-0
Done
Copy file /slot1/tmp-lp-monitor-0 on MP to file monitor on all LP slots
.....File Download: /slot1/tmp-lp-monitor-0 (MP) -> monitor (LP 1) is done.
.File Download: /slot1/tmp-lp-monitor-0 (MP) -> monitor (LP 3) is done.
File Download: /slot1/tmp-lp-monitor-0 (MP) -> monitor (LP 2) is done.
File download to interface module is done (3 successful)

3) Install MP application image /Application/ManagementModule/xmr06300aa.bin from tftp
10.20.81.154 to primary:
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
............................Verified OK
FIPS: Image verification passed for primary

SYSLOG: <14>Aug  9 2019 19:42:58 FIPS: Image verification passed for primary
Done

4) Install LP application image /Application/InterfaceModule/xmlp06300aa.bin from tftp
10.20.81.154 to primary:
Save a copy to MP's flash, please
wait.....................................................................................
.....................................................................................
.....................................................................................
.....................................................................................
.....................................................................................
.....................................................................................
.....................................................................................
.............Verified OK
```

```
FIPS: Image verification passed for lp-primary-0

SYSLOG: <14>Aug  9 2019 19:44:02 FIPS: Image verification passed for lp-primary-0
Done
Copy file /slot1/tmp-lp-primary-0 on MP to file primary on all LP slots
.....................................................................File Download: /
slot1/tmp-lp-primary-0 (MP) -> primary (LP 1) is done.
.......File Download: /slot1/tmp-lp-primary-0 (MP) -> primary (LP 3) is done.
.File Download: /slot1/tmp-lp-primary-0 (MP) -> primary (LP 2) is done.
File download to interface module is done (3 successful)

5) Bundle LP FPGA skipped, same FPGA versions exist.

SYSLOG: <14>Aug  9 2019 19:45:20 Single-command upgrade completed successfully.

System Upgrade Done.
Upgrade Summary
  Source: tftp 10.20.81.154 Directory
1) Installed /Monitor/ManagementModule/xmb06200.bin to MP Monitor
2) Installed /Monitor/InterfaceModule/xmlb06200.bin to LP Monitor on all LP slots
3) Installed /Application/ManagementModule/xmr06300aa.bin to MP Primary
4) Installed /Application/InterfaceModule/xmlp06300aa.bin to LP Primary on all LP slots
5) Skipped /Combined/FPGA/lpfpga06300aa.bin to LP FPGA Bundled, same versions exist.

Checking for coherence...
Done.
device#
```

Firmware Version Installed

The installed firmware version can be displayed from the CLI using **show version** command. The string following "labeled as" is the version number and not the string following the word "Version" in the output of the command. Examples of version numbers are highlighted in the output examples that follow.

For Extreme NetIron CER device:

```
device# show version
      NetIron CER 2024C-4X#show versionSystem: NetIron CER (Serial #: CKO2531J36C,  Part
#:
      40-1000860-13)License: RT_SCALE, ADV_SVCS_PREM (LID: emqHKIGlILe)Boot     : Version
6.0.0T185 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Jun  7 2016 at 16:10:10 labeled as ceb06000(465568 bytes) from boot
flashMonitor  : Version 6.0.0T185 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Jun  7 2016 at 16:10:10 labeled as ceb06000(465568 bytes) from code
flashIronWare : Version 6.3.0aT183 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Jul 12 2019 at 18:16:56 labeled as ce06300aa(18718042 bytes) from
PrimaryCPLD Version: 0x00000001Micro-Controller Version: 0x0000000dExtended route
scalabilityPBIF Version: 0x0162800 MHz Power PC processor 8544 (version 8021/0023) 400 MHz
      bus512 KB Boot Flash (MX29LV040C), 64 MB Code Flash
      (MT28F256J3)2048 MB DRAMSystem uptime is 3 minutes 6 seconds
```

Note

The software version number is tracked by "labeled as". For CER the version, for example, is "ce06300aa". The text after "Version" is used for internal system purpose only. Version numbers are highlighted in the outputs of the **show version** commands for clarity.

xmprm05900: Version number of the boot image on the Management module.

xmb06200: Version number of the monitor image on the Management module.

xmr06300aa: Version number of the MP application image.

For Extreme MLXe device management module:

```
device# show version
System Mode: MLXChassis:
MLXe 4-slot (Serial #: BGD2547F02N,  Part #:40-1000363-03)NI-X-HSF Switch Fabric Module 1
(Serial #: BEW0338F01Z, Part #:60-1001512-09)FE 1: Type fe600,  Version 1 Switch Fabric
Module 1 Up Time is 2 days 23 hours 41 minutes 18 seconds
NI-X-HSF Switch Fabric Module 2 (Serial #: BEW0338F00M,  Part #: 60-1001512-09)FE 1: Type
fe600,  Version 1 Switch Fabric Module 2 Up Time is 2 days 23 hours 41 minutes 18 seconds
NI-X-HSF Switch Fabric Module 3 (Serial #: BEW0335F04M,  Part #: 60-1001512-10)FE 1: Type
fe600,  Version 1 Switch Fabric Module 3 Up Time is 2 days 23 hours 41 minutes 18 seconds

================================================================================
SL M1: BR-MLX-MR2-X Management Module Active (Serial #: BVR2505J02G, Part
      #: 60-1002375-06):Boot     : Version 5.9.0T165 Copyright (c) 2017-2019 Extreme
Networks,
      Inc.Compiled on Mar 19 2015 at 03:16:46 labeled as xmprm05900(521771 bytes) from
boot flashMonitor  : Version 6.2.0T165 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Aug 17 2017 at 11:22:12 labeled as xmb06200(546965 bytes) from code
flashIronWare : Version 6.3.0aT163 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Apr 18 2019 at 16:17:08 labeled as xmr06300aa(10800652 bytes) from
PrimaryBoard ID : 00 MBRIDGE Revision : 371666 MHz Power PC processor 7448 (version
8004/0202) 166 MHz
      bus512 KB Boot Flash (MX29LV040C), 128 MB Code Flash
      (MT28F256J3)4096 MB DRAM INSTALLED4096 MB DRAM ADDRESSABLEActive Management uptime
is 2 days 23 hours 41 minutes 18 seconds

================================================================================
SL M2: BR-MLX-MR2-X Management Module Standby (Serial #: BVR2511H016, Part
      #: 60-1002375-06):Boot     : Version 5.9.0T165 Copyright (c) 2017-2019 Extreme
Networks,
      Inc.Compiled on Mar 19 2015 at 03:16:46 labeled as xmprm05900(521771 bytes) from
boot flashMonitor  : Version 6.2.0T165 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Aug 17 2017 at 11:22:12 labeled as xmb06200(546965 bytes) from code
flashIronWare : Version 6.3.0aT163 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Apr 18 2019 at 16:17:08 labeled as xmr06300aa(10800652 bytes) from
PrimaryBoard ID : 00 MBRIDGE Revision : 371666 MHz Power PC processor 7448 (version
8004/0202) 166 MHz
      bus512 KB Boot Flash (MX29LV040C), 128 MB Code Flash
      (MT28F256J3)4096 MB DRAM INSTALLED4096 MB DRAM ADDRESSABLEStandby Management uptime
is 2 days 23 hours 40 minutes 24 seconds

================================================================================
SL 1: BR-MLX-10Gx20 20-port 1/10GbE Module (Serial #: CWB0411L01N, Part #:
      60-1002946-12)License: 20x10G-WITH-1G-MODE-ONLY, 20x10GbE-X2-Scaling-UPG (LID:
      eydFJGGnFGp)Boot     : Version 5.9.0T175 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Mar 19 2015 at 03:17:00 labeled as xmlprm05900(449576 bytes) from
boot flashMonitor  : Version 6.2.0T175 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Aug 17 2017 at 11:22:42 labeled as xmlb06200(573366 bytes) from
code flashIronWare : Version 6.3.0aT177 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Apr 18 2019 at 16:45:30 labeled as xmlp06300aa(9537274 bytes) from
PrimaryFPGA versions:Valid PBIF Version = 2.11, Build Time = 8/19/2016 14:54:00 Valid XPP
Version = 0.00, Build Time = 9/22/2017 11:27:00 MACXPP100G 0MACXPP100G 11199 MHz MPC
P2010 (version 8021/1051) 599 MHz bus512 KB Boot Flash (MX29LV040C), 66846720 Bytes (~64
MB) Code Flash
      (MT28F256J3)3072 MB DRAM, 8 KB SRAMLP Slot 1 uptime is 2 days 23 hours 40 minutes
25 seconds

================================================================================
SL 2: BR-MLX-10Gx20 20-port 1/10GbE Module (Serial #: CWB0449K0CD, Part #:
      60-1002946-12)License: 20x10GbE-X2-Scaling-UPG (LID: eydFJJOmFef)Boot     : Version
5.9.0T175 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Mar 19 2015 at 03:17:00 labeled as xmlprm05900(449576 bytes) from
boot flashMonitor  : Version 6.2.0T175 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Aug 17 2017 at 11:22:42 labeled as xmlb06200(573366 bytes) from
```

```
code flashIronWare : Version 6.3.0aT177 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Apr 18 2019 at 16:45:30 labeled as xmlp06300aa(9537274 bytes) from
PrimaryFPGA versions:Valid PBIF Version = 2.11, Build Time = 8/19/2016 14:54:00 Valid XPP
Version = 0.00, Build Time = 9/22/2017 11:27:00 MACXPP100G 0MACXPP100G 11199 MHz MPC
P2010 (version 8021/1051) 599 MHz bus512 KB Boot Flash (MX29LV040C), 66846720 Bytes (~64
MB) Code Flash
      (MT28F256J3)3072 MB DRAM, 8 KB SRAMLP Slot 2 uptime is 2 days 23 hours 40 minutes
26 seconds

==========================================================================
SL 3: BR-MLX-10Gx4-M-IPSEC 4-port 1/10GbE and 4-port 1GbE Module (Serial #:
      CWH0451K00F, Part #: 60-1002974-12)Boot     : Version 5.9.0T175 Copyright (c)
2017-2019 Extreme Networks,
      Inc.Compiled on Mar 19 2015 at 03:17:00 labeled as xmlprm05900(449576 bytes) from
boot flashMonitor  : Version 6.2.0T175 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Aug 17 2017 at 11:22:42 labeled as xmlb06200(573366 bytes) from
code flashIronWare : Version 6.3.0aT177 Copyright (c) 2017-2019 Extreme Networks,
      Inc.Compiled on Apr 18 2019 at 16:45:30 labeled as xmlp06300aa(9537274 bytes) from
PrimaryFPGA versions:Valid PBIF Version = 2.11, Build Time = 8/19/2016 14:54:00 Valid XPP
Version = 0.00, Build Time = 4/13/2017 16:22:00 XGMAC-2 0XGMAC-2 1XGMAC-2 2XGMAC-2 31199
MHz MPC P2010E (version 8021/1051) 599 MHz bus512 KB Boot Flash (MX29LV040C), 66846720
Bytes (~64 MB) Code Flash
      (MT28F256J3)3072 MB DRAM, 8 KB SRAMLP Slot 3 uptime is 2 days 23 hours 40 minutes
23 seconds
==========================================================================
```

Setting System Time and Date

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

device# clock set hh:mm:ss mm-dd-yy

where

hh:mm:ss mm-dd-yy

Specifies the local clock time and date in hours, minutes, seconds, month, day and year. Valid date and time settings range from January 1, 1970 to January 19, 2035.

Note
The use of NTP is not allowed in a Common Criteria configuration.

Banner commands

The following commands are used to configure banner messages. The banner messages are used to provide information to the user when the TOE is accessed.

- Banner incoming: sets the incoming banner message. The message is seen on the console when a user accesses the device.
- Banner motd: sets the message of the day banner. The message is displayed when the device receives a login request.

The range of banner length is from 1 to 2048 characters. Characters can be issued as a single line of text bracketed by a start character and the same character at the end.

These commands can be invoked from the CLI in configuration mode.

```
device # banner incoming x <message> x
```

where **x** can be any printable character.

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

Configuring authentication in the devices

About This Task

To configure the authentication in the switches, use the following steps:

Procedure

1. Configure the username and password with privilege by using the following command,

   ```
   device(config)# username <username> privilege <0> password
   (Enter new password:)*******
   ```

   Note
   Each privilege has roles defined. For example: 0: read/write, 4: port configuration, 5: Read only.

2. Use following configuration to configure different authentication methods (Radius, Local):

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

3. Use following configuration to configure one or more Radius servers:

   ```
   device(config)# radius-server host <ip> ssl-auth-port <ssl-port> default key
   <keystring>
   ```

TLS client mode: Authenticating server certificate

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

- Certificate validation and the certificate path validation support a minimum path length of three certificates.
- The certificate path must terminate with a trusted CA certificate.
- The certificate path should be validated by verifying the presence of the `basicConstraints` extension and that the CA flag is set to TRUE for all CA certificates.
- The revocation status of the certificate should be validated using the Online Certificate Status Protocol (OCSP).
- The `extendedKeyUsage` field should be validated according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification should have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the `extendedKeyUsage` field.
  - Server certificates presented for TLS should have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the `extendedKeyUsage` field.
  - Client certificates presented for TLS should have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the `extendedKeyUsage` field.
  - OCSP certificates presented for OCSP responses should have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the `extendedKeyUsage` field.
- A certificate should only be treated as a CA certificate if the `basicConstraints` extension is present and the CA flag is set to TRUE.

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

TLS cipher suites for client and server applications

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

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

Verify the revocation status of certificate using OCSP

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

When the switch cannot establish a connection to determine the validity of a certificate, then it will not accept the certificate. If the digital certificate does not have authorityInfoAccess extension with an OCSP URI, then no revocation check is performed on that certificate.

OCSP support for TLS

OCSP maintains the security of the server and other network resources. OCSP send a request for certificate status information to the server and recieves back a response of current, expired or unknown. The protocol specifies the communication between server and the client applicatio n. OCSP allows expired certificates with a grace period to access servers for a limited time before renewing.

During TLS handshake, when TLS client recieves the server certificate with OCSP information, the TLS or OCSP client can request for the OCSP responder for the validity of the certificate.The certificate status can be valid or revoked.

This feature supports x509v3 certificate validity using the OCSP protocol in accordance with RFC 6960. The OCSP request contains:

- The OCSP encoded as zero (0)
- The signature algorithm used in the request.
- Certificate's issuer distinguished name.

- Certificate's issuer public key
- Certificate's serial number

The OCSP response provides the certificate revocation status to the client with the following options:

- Good: Indicates that requested certificate serial number within its validity in not revoked.
- Revoked: Indicates the certificate has been revoked, either temporarily or permanently.
- Unknown: Indicates the certificate being requested was not recognized or there was a failure in the HTTP connection with the OCSP responder.

When OCSP is enabled for TLS, it is important to ensure that the OCSP Responder supports SHA256 hash algorithm and HTTP POST method.

Application timer

When TLS is used with OCSP during chain certificate validation or when stunnel is used as proxy TLS server a non-secure application, it is recommended to maximize the connection timeout of the server. RADIUS timeout can be set to a maximum value of 12 seconds using the following command.

```
device# aaa accounting exec default start-stop radius
device# aaa authentication login default radius local-auth-fallback
radius-server host <Radius Server Ip> ssl-auth-port <Port number to communicate to the
radius server> default key < Radius Secret Key>
radius-server timeout < in seconds>
```

TACACS+ timeout can be set to a maximum value of 15 seconds using the following command:

```
tacacs-server timeout < in seconds>
```

To import the certificate from the server, use the following command:

```
scp ca.cert.pem <switch username>@<Switch Management IP>:ssltrustedcert
```

Configuring SSH session rekey interval by volume and time

SSH servers can trigger rekeying once a certain time interval is reached or data traffic reaches a specified volume. During rekeying, a set of key exchange messages are transferred between the SSH client and the server, changing the key used for the session security.

Rekeying by volume

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

The range of the rekey volume configured using the **ssh-server** command is 50 to 1024 MB.

```
device(config)# ip ssh server rekey-volume ?
Possible completions:
  <DECIMAL>   <50-1024> Megabytes"
```

Rekeying by time

The time limit must be set to a value for SSH rekey that is less than 60 minutes to be compliant with Common Criteria. Values of 3600 seconds or higher must not be used. The following command can be used to specify the time.

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

Login inactivity timeout values

To set the value on Console

```
device(config)#console timeout ?
  DECIMAL   <0..240> In minutes, 0 never timeout
```

To configure the idle timeout for SSH

This is the idle timeout of SSH session. The session will disconnect if there is inactivity in the session for the specified period.

```
device(config)#ip ssh idle-time ?
  DECIMAL   <0-240> minutes, 0 never timeout
```

Syslog configuration

The native Syslog client on the switch needs to know the location of a remote Syslog server. For that the server details needs to be configured on the device.

1. To configure the IP address and TLS port of the server use the following command:

   ```
   device(config)# logging host <ip> ssl-port <number>
   ```

   Note
   The <ip> is the reference identifier that identifies the IP address of the Syslog server, and must be represented in the CN or SAN field of the digital certificate presented by the server during TLS connection establishment.

2. TLS client on the device have the trusted root CA for any authentication of the X.509v3 digital certificate presented by the TLS server while the connection is being setup. Each TLS server's trusted root CA certificate has to be preinstalled on the device. The TLS server itself may be encapsulating high level audit protocol like Syslog, or authentication protocols like RADIUS or TACACS+. In order to install the root CA certificate, use the following command from the remote server that has the X.509v3 certificate installed:

   ```
   Remote# scp <root cert> user@<mlx ip>:ssltrustedcert
   ```

   There are three Root CA certificates which can be added to the device. Each Root CA imported to the device can be used by all the TLS server applications (Syslog, RADIUS, TACACS+), or Each Root CA can be used for each TLS server applications. None of the imported Root CA certificate is tied to any specific application.

   Note
   SCP command is applicable to all TLS server applications (Syslog, RADIUS, TACACS+).

3. To process the received Syslog message, and this can be in various ways. For instance, user may save it to a local file, forward to another application, or another host in the network.

The device disconnects from the the Syslog server, if the device does not have audit data to transmit for the default value of 132 minutes (2 hours and 12 minutes) which is based on the underlying TCP keepalive interval. There is no support to modify this timeout value. If the connection is lost, the Syslog client on the device will retry to establish the connection.

To have a successful handshake between certificate and TLS, consider following assumptions for the Syslog server.

1. It contains and sends the server certificate and corresponding intermediate CA certificate which signed the server certificate.
2. It supports TLS version 1.1 and higher.
3. It supports at-least one of the client supported cipher-suit.

Encrypted Syslog servers in Common Criteria mode

NetIron devices in any mode send the generated Syslog messages in real time to the local log storage on the device and to a Syslog server (only if a Syslog server is configured and available).

A NetIron device running in Common Criteria operational mode queues the Syslog messages if a Syslog server is not available or configured for the device. The max configurable limit is 5000 and default is 500 Syslog messages. When the configured maximum limit is reached, new audit logs will replace the first audit log and for every new audit logs it will replace every subsequent existing audit logs.

Syslog buffer limit can be configured by following command:

```
device(config)#logging buffered ?
  DECIMAL         <1..5000> Dynamic log entries
  alerts          Enable/disable logging of alert messages
  critical        Enable/disable logging of critical messages
  debugging       Enable/disable logging of debugging messages
  emergencies     Enable/disable logging of emergency messages
  errors          Enable/disable logging of error messages
  informational   Enable/disable logging of informational messages
  notifications   Enable/disable logging of notification messages
  warnings        Enable/disable logging of warning messages
device(config)#logging buffered 5000
```

NetIron devices, when enabled for Common Criteria mode, do not support Syslog servers that use UDP transport. However, other parameters that are defined for Syslog server connections, such as specifying the hold time for queued messages and traps when the device reloads or switches over are applicable for encrypted Syslog connections as well.

When you enable Common Criteria mode on a device, the device is in the Common Criteria Administrative mode, where Syslog server configuration that uses UDP transport is retained. You can configure encrypted Syslog server connections in this mode. However, Syslog messages that are generated when the device is in the administrative mode are sent to the UDP Syslog servers, not to the encrypted Syslog server that you have configured. When the device is put in the Common Criteria Operational mode, existing Syslog servers that use UDP transport are removed, and only encrypted Syslog server connections are accepted.

Conversely, when a device is downgraded from Common Criteria mode, the encrypted Syslog server connections that were configured are removed, and the device supports only unencrypted UDP Syslog servers. The following table summarizes these transitions.

Table 7: Syslog server connections during transition to and from Common Criteria mode

From	To non-FIPS mode	To FIPS mode	To Common Criteria Operational mode
Non-FIPS mode	Not applicable	No change. FIPS mode does not require encrypted Syslog servers.	All the UDP servers are removed when the device is put in CC Operational mode. Only encrypted Syslog server connections are allowed in CC Operational mode.
FIPS mode	No change	Not applicable	All the UDP servers are removed when the device is put in CC Operational mode. Only encrypted Syslog server connections are allowed in CC Operational mode.
Common Criteria mode	All the SSL servers are removed. Non-FIPS mode does not support encrypted Syslog server connections.	Not allowed. You must disable Common Criteria mode to revert to non-FIPS mode, and then re-enable FIPS mode. FIPS mode does not support encrypted Syslog server connections.	Not applicable

AAA servers in Common Criteria mode

Common Criteria mode requires that devices support NDcPP version 2.1. This protocol defines the communication of the device with AAA servers to take place over a TLS support session.

Even though you can configure multiple TLS support for TACACS+ or RADIUS servers, only one connection can be active at any time due to system limitations. If another TLS support for TACACS+ or RADIUS session is attempted at the same time as the first TACACS+ or RADIUS session, the connection attempt is rejected.

Additionally, since the TACACS+ or RADIUS server may accept only a single TACACS+ or RADIUS session over the TCP or the TLS support connection, it is recommended you use this only for authentication.

When the device is in Common Criteria Operational mode, and the device has been configured for a TLS support for TACACS+ or RADIUS server for authentication, only one administrator will be able to administer the device. In addition, accounting and authorizing using the TLS support for TACACS+ or RADIUS server will be disabled.

Following are the configuration commands to configure and use a RADIUS server over secure port.

```
device(config)# aaa authentication login default radius
device(config)# aaa authorization commands 0 default radius
device(config)# aaa accounting commands 0 default start-stop radius
device(config)# radius-server host 10.24.12.107 ssl-auth-port 2083 default key Pass@123
```

For **`radius-server host`** command, 10.24.12.107 is the IP address of the radius server listening on secure port 2083 and has been configured with shared secret Pass@123 in the server configuration. Refer to the configuring a RADIUS server with TLS support for details on RADIUS server configuration.

When the RADIUS timeout is not configured, the default timeout of 3 seconds is used to establish connection to a server. When you use stunnel as TLS proxy server between the device and RADIUS server the timeout should be increased to atleast 6 seconds.

```
device(config)#radius-server timeout 6
```

Note

You can modify the default Common Criteria policy to allow a non-TLS support for TACACS+ or RADIUS server, but this will make the device noncompliant with Common Criteria requirements.

For configuring TACACS+, use the following commands:

```
device(config)#aaa authentication login default tacacs+ local
 device(config)#aaa authentication login privilege-mode
device(config)#tacacs-server host 10.24.12.107 ssl-auth-port 60591 authentication-only
key My$ecret123
device(config)#tacacs-server timeout 15
```

10.24.12.107 is the TACACS+ server listening on TLS port 60591 and configured with secret key My $ecret123. Unlike RADIUS, TACACS+ server has not been validated with native support for TLS on the server side and stunnel proxy server has been used. The maximum recommended TACACS+ connection timeout is 15.

More than one server can be configured on device for both RADIUS and TACACS+ servers . The device connects to them in series depending on the order of configuration. If it is able to connect to a server then it does not connect to subsequent servers.

Verify the revocation status of certificate using OCSP

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

When the switch cannot establish a connection to determine the validity of a certificate, then it will not accept the certificate. If the digital certificate does not have authorityInfoAccess extension with an OCSP URI, then no revocation check is performed on that certificate.

Downgrading from Common Criteria mode to non-FIPS mode

Downgrading a device from Common Criteria mode to either FIPS mode or non-FIPS mode uses the same command. You cannot directly downgrade to FIPS mode; you first downgrade to non-FIPS mode, and then enable FIPS mode using the procedures detailed in the earlier chapter.

About This Task

After the device is placed in non-FIPS mode, you can use SCP to download and initialize an older image. Use the following steps to revert to a non-FIPS-compliant image.

Procedure

1. Log in to the device by entering your username and password.
2. Disable Common Criteria mode by entering the **`no fips enable`** or **`no fips enable common-criteria`** command.
3. Regenerate SSH host keys or other shared secrets as needed for access after reload.
4. To replace the startup configuration with the **`no fips enable`** configuration, enter the **`write memory`** command.
5. Reload the configuration by entering the **`reload`** command.

OpenSSL License

OpenSSL license overview on page 37

OpenSSL license overview

Note
This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

Note
OpenSSL has been compiled without the Heartbeat extension.

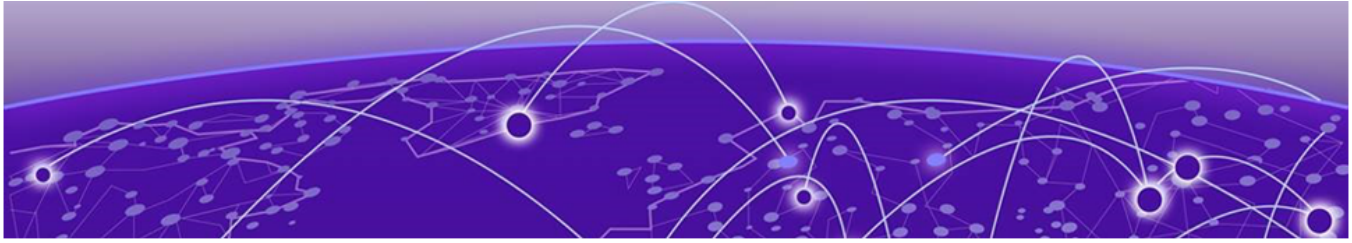
License

This is a copy of the current LICENSE file inside the CVS repository.

```
LICENSE ISSUES
==============
The OpenSSL toolkit stays under a double license, i.e. both the conditions of
  the OpenSSL License and the original SSLeay license apply to the toolkit.
  See below for the actual license texts. Actually both licenses are BSD-style
  Open Source licenses. In case of any license issues related to OpenSSL
  please contact openssl-core@openssl.org.

  OpenSSL License
  ---------------

/* ====================================================================
* Copyright (c) 1998-2018 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
 *
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
```

```
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License
-----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
 * This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to.  The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code.  The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
 * Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
 * Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*    notice, this list of conditions and the following disclaimer.
```

```
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in the
*    documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*    must display the following acknowledgement:
*    "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*    The word 'cryptographic' can be left out if the rouines from the library
*    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
*    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
 * The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed.  i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```



Appendix A - Audit Log Entries

The following tables list some of the notable log entries.

Audit Logs

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

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

The entries are displayed in the following format:

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

Where:

Timestamp is when an event is recorded in the log.

Entry Number is the item number in the log

Entry type is the type of the audit log item, in this example, an informational entry recorded by a security-related event

Access Method is how this event triggered and the access used for this event, the 5-tuple includes the user name, privilege and how the device is being accessed (e.g., CLI or none if through a protocol transition)

Device Name is the TOE

Event is the security-related trigger for this entry

Event Description contains additional information regarding the event

The log can be displayed from the CLI by:

```
device# show logging auditlog
```

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

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

CLI Audit

CLI Audit can be enabled using configuration command:

```
device(config)# logging cli-command
```

This command causes the TOE to audit all commands administered through the CLI. The audit log generated will contain the command entered by the administrator. Please note that help commands are not audited as well as invalid commands (e.g., incorrect syntax).

Following is a sample CLI log message:

Sample Log	Log Description
Aug 14 01:19:07:I:CLI CMD: "fips show " from ssh client 192.168.1.1	<timestamp>: CLI CMD: "<command>" from [console | telnet client <client-ip> | ssh client <client ip>]

TLS-related audit log entries

Table 8: TLS-related audit log entries

Operation	Log details
TLS session establishment	Oct 9 08:34:45:W: TLS: Successfully TLS connection established for10.24.12.107:60892
TLS session termination (client/server)	Oct 9 08:34:51:W: TLS: TLS Connection terminated successfully for10.24.12.107:60892
Invalid TLS version(after this entry, the TLS Session Termination log is also displayed) Major# represents the hexa-decimal value in the packet for invalid TLS major version	Oct 9 08:34:51:W: TLS: INVALID TLS version Major <Major #> from 10.24.12.107:60892
Invalid TLS cipher (after this entry, the TLS Session Termination log is also displayed)	Oct 9 08:36:23:W:TLS: No Matching Cipher

Table 8: TLS-related audit log entries (continued)

Operation	Log details
Unsupported TLS version. Minor # represents the hexa decimal value in the packet for TLS minor version	Oct 9 08:45:43:W: TLS: Not enabled TLS version 1.<Minor #> from 10.24.12.107:60892
Decryption Failed	Oct 9 09:02:45:W:TLS Handshake: Decryption Failed for 10.24.12.107:60892
Bad record MAC	Oct 9 08:34:45:W:TLS Handshake: Bad record MAC- invalid padding for 10.24.12.107:60892
Invalid server EKU being used	Oct 9 09:14:08:W:TLS X509v3 Certificate Validation failed: unsupported certificate purpose from 10.24.12.107:60892
Wrong server EKU being used	Oct 9 09:15:15:W:TLS: Wrong Extended Key Usage value for 10.24.12.107:60982
Key exchange message of an invalid type	Oct 9 09:16:25:W:TLS: Key Exchange or signature invalid type for 10.24.12.107:60982
Unexpected message (Finished message sent before the ChangeCipherSpec message)	Oct 9 09:17:15:W:TLS: TLS Handshake: Finished message processing error from 10.24.12.107:60982
Syslog server connected on TLS	May 14 17:09:07 mlxe System: SSL Syslog server 172.16.16.254:6514 is now active Syslog server Operation
Syslog server on TLS is disconnected	May 14 17:18:45 mlxe System: SSL Syslog server 172.16.16.254:6514 is disconnected. Note: This log will occur every minute if TLS Syslog server is configured on device but not running remotely i.e, when connection attempt fails Operation.
TLS Handshake error	Jun 27 23:45:49 mlxe TLS: TLS Connection had received error to terminate from server 172.16.16.254:1492 during handshake Note: This log will occur every minute if TLS Syslog server is configured on device but not running remotely i.e, when connection attempt fails.
TLS Signature algorithm mismatch	Oct 9 08:34:45:W: X509v3 Certificate Validation failed: signature algorithm
SAN doesn't exist and CN doesn't match	Oct 9 08:34:45:W: TLS: SAN doesn't exist and CN doesn't match server IP <IP addr>:<port> CN <IP in CN field>
SAN exist and doesn't match	Oct 9 08:34:45:W: TLS: SAN available but doesn't match server IP <IP addr>:<port> SAN <IP in SAN field>
TLS certificate expired	Oct 9 08:34:45:W: TLS: Certificate validity from <IP addr>:<port> is expired.
Import X509v3 root certificate	Oct 9 08:34:45:W: SCP: Download by admin from src IP <remote IP addr> to ssl trusted certificate. Oct 9 08:34:45:W: SCP: TLS Trusted certificate downloaded successfully to dynamic trusted index <index>

OCSP and Certificate-related Audit Log entries

Note
The certificate index mentioned below follows the order in chain like server certificate has index 1, issuer of server certificate has index 2 and issuer of the issuer has index 3 and so on.

Table 9: OCSP and Certificate-related Audit Log entries

Operation	Log Details
Certificate contains OCSP URI, but device encountered error in parsing	Jan 9 22:51:51:E:Failed to parse responder IP=<junk data when parsing> URL from cert
OCSP Responder is not reachable	Jan 9 22:51:51:E:OCSP: Responder was not reachable due to error status
Certificate status is unknown	Jan 9 22:51:51:E:OCSP: Server/Intermediate Certificate of Index 2 in the chain is unknown
Certificate status if revoked	Jan 9 22:51:51:E:OCSP: Server/Intermediate Certificate of Index 1 in the chain is revoked
OCSP responder is reachable but returns failure	Jan 9 22:51:51:E:OCSP: Http error 201 returned from responder

OCSP responder returned invalid response status	Jan 9 22:51:51:E:OCSP:The following are the various response status codes. This audit log will be filed for all statuses. except 0.
	`successful (0) - Response has valid confirmations`
	`malformedRequest (1) - Illegal confirmation request`
	`internalError (2) - Internal error in issuer`
	`tryLater (3) - Try again later`
	`(4) - not used`
	`sigRequired (5) - Must sign the request`
	`unauthorized (6) - Request unauthorized`
	`Eg OCSP: Response status 1 is invalid`

OCSP responder returned response type in the packet not matching basic	Jan 9 22:51:51:E:OCSP:Response type is not OCSP basic
OCSP responder returned version not matching 0	Jan 9 22:51:51:E:OCSP: Response version is invalid
OCSP responder returned repsonder tag not matching 1 or 2	Jan 9 22:51:51:E:OCSP: Responder id tag 0 is invalid
OCSP responder sent a certificate whose thisUpdate time has expired	Jan 9 22:51:51:E:OCSP: Response has expired
OCSP responder sent a response where the signature algorithm is not SHA256	Jan 9 22:51:51:E:OCSP: Response does not have responder certificate or data mismatch for responder tag <responder tag>
OCSP responder sent responder id tag as 1, but cert DN and responder data are not same	Jan 9 22:51:51:E:OCSP:Response does not have responder certificate or data mismatch for responder tag <responder tag>

Table 9: OCSP and Certificate-related Audit Log entries (continued)

Operation	Log Details
OCSP responder sent responder id tag as 2, but cert public key hash and responder data don't match	Jan 9 22:51:51:E:OCSP:Response does not have responder certificate or data mismatch for responder tag <responder tag>
OCSP responder sent a certificate whose ASN parsing failed on the switch	Jan 9 22:51:51:E:OCSP: Responder certificate is invalid
OCSP responder sent a certificate without EKU field	Jan 9 22:51:51:E:OCSP: Responder certificate EKU field is NULL
OCSP responder sent a certificate without EKU field assigned to signing purpose	Jan 9 22:51:51:E:OCSP: Responder certificate EKU field is not set to OCSP signing purpose
OCSP responder sent a response without responder certificate or data mismatch	Jan 9 22:51:51:E:OCSP: Response does not have responder certificate or data mismatch for responder tag <responder tag>

SSH related audit log entries

Table 10: SSH related audit log entries

Operation	Log Details
SSH Successful Login	Jan 17 11:18:59:I:Security: SSH login by Test_1234 from src IP 10.6.40.119 to USER EXEC mode using RSA as Server Host Key
SSH Failed login attempt	Jan 17 11:20:39:I:Security: SSH access by user abc from src IP 10.6.40.119 rejected, 1 attempt(s)
SSH logout record/Inactivity timeout (Used by netconf as well)	Jan 17 11:20:17:I:Security: SSH logout by Test_1234 from src IP 10.6.40.119 from USER EXEC mode using RSA as Server Host Key
Login timeout occurred on SSH session	Jan 17 11:30:31:I:SSH: SSH disconnect due to login timeout for session from client 10.24.12.107 session id 0
Server hostkey change via CLI	Jan 17 11:16:19:I:CLI CMD: "crypto key generate rsa modulus 2048" from console eg: Jan 17 11:16:18:I:Security: SSH Server RSA as Server Host Key enabled by operator from console session
Idle timeout change via CLI	Jan 17 11:30:15:I:CLI CMD: "ip ssh idle-time 235" from console
Authenticated retries change via CLI	Jan 17 11:30:31:I:CLI CMD: "ip ssh authentication-retries 4" from console
Encryption algorithm change via CLI	Jan 17 11:40:20:I:CLI CMD: "ip ssh encryption aes-only" from console
Invalid hostkey	Jan 17 11:40:20:E:SSH: Invalid hostkey algorithm recieved from client 10.24.12.107 session id 0 algorithm received ssh-dsa
Invalid key-exchange algorithm	Jan 17 11:40:20:E:SSH: Invalid key exchange algorithm recieved from client 10.24.12.107 session id 0 algorithm received diffie-hellman-group-exchange-sha256

Table 10: SSH related audit log entries (continued)

Operation	Log Details
Invalid cipher algorithm	Jan 17 11:40:20:E:SSH: Invalid cipher algorithm received from client 10.24.12.107 session id 0 algorithm recieved aes-256cbc
Invalid MAC algorithm	Jan 17 11:40:20:E:SSH: Invalid mac algorithm recieved from client 10.24.12.107 session id 0 algorithm received hmac-sha2-512
Invalid packet received	Jan 17 11:40:20:W:SSH: SSH: Packet of invalid length not within range of buffer received from client 10.10.10.1 session id 0
Rekey triggered due to rekey interval expiry	Jan 17 11:40:20:I:SSH: Going for rekeying since rekey interval = 900 seconds expired for client 10.24.12.107 session id 0
Rekey triggered due to packet volume expiry	Jan 17 11:40:20:I:SSH: Going for rekeying since rekey volume = 50 megabytes expired for client 10.24.12.107 session id 0
Login timeout occurred on SSH session	Jan 17 11:40:20:I:SSH: SSH disconnect due to login timeout for session from client 10.24.12.107 session id 0
Import an SSH public key	Jun 13 17:14:19 cer2024 SCP: Download by admin from src IP 172.16.16.254 to ssh public key. Jun 13 17:14:19 cer2024 SCP: SSH Public key file downloaded successfully.
Delete an SSH public key	Jun 13 16:31:41 cer2024 CLI CMD: "ip ssh pub-key remove" by admin from ssh client 172.16.16.254
SSH timeout	Jun 17 17:36:16 cer2024 Security: ssh timed out by admin from src IP 172.16.16.254 from USER EXEC mode using RSA as Server Host Key

Certificate audit log entries

Table 11: Certificate audit log entries

Operation	Log Details
The issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found	Oct 9 09:21:19:W: TLS: Issuer certificate is not available
The public key in the certificate SubjectPublicKeyInfo could not be read	Oct 9 09:21:19:W: X509v3 Certificate Validation failed: parse error on public key
The certificate is not yet valid: the notBefore date is after the current time	Oct 9 09:21:19:W:TLS : X509v3 Certificate Validation failed: parse error on notBefore
The certificate has expired: that is the notAfter date is before the current time	Oct 9 09:21:03:W:TLS :X509v3 Certificate Validation failed: parse error on notAfter
The certificate common name doesn't match with server's IP address	Oct 9 09:21:03:W: TLS: IP in certificate doesn't match SAN
The basicConstraints parameter is false for CA certificate	Oct 9 09:22:08:W:TLS: BasicConstraints_CA is False for CA cert
The basicConstraints parameter is absent for CA certificate	Oct 9 09:23:11:W:TLS:X509v3 Certificate Validation failed: basic constraints absent for CA certificate %s
The certificate notBefore field contains an invalid time	Oct 9 10:11:35:W:TLS: Certificate validity is ahead of the current time

Table 11: Certificate audit log entries (continued)

Operation	Log Details
The certificate notAfter field contains an invalid time	Oct 9 11:00:42:W:TLS: Certificate validity is ahead of the current time
The certificate chain could be built up using the untrusted certificates but the root could not be found locally	Oct 29 13:20:31.835 Error: Certificate chain doesn't end with any trusted certificate
The basicConstraints path-length parameter has been exceeded	Oct 9 11:03:52:W:TLS :X509v3 Certificate Validation failed: path length constraints exceeded
The certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value, this is only meaningful for RSA keys	Oct 9 11:03:52:W: X509v3 Certificate Validation failed: parse error on signature algorithm
Signature algorithm mismatch	Oct 9 12:34:45:W:TLS: X509v3 Certificate Validation failed: signature algorithm mismatch
Signature key length is invalid	Oct 9 12:34:45:W:TLS: X509v3 Certificate Validation failed: signature algorithm key is too big
TLS: In FIPS CC mode Minimum 2 certificates are needed excluding the trusted certificate	Oct 9 12:24:49:W:TLS: In FIPS CC mode Minimum 2 certificates are needed excluding the trusted certificate
During trusted CA import device failed to retrieve the size of the file	Oct 9 11:03:52:W: TRUSTED CERT IMPORT: Failed to retrieve the size of the certificate file
During trusted CA import device failed to read the file from flash	Oct 9 11:03:52:W: TRUSTED CERT IMPORT: Failed to read certificate file from flash
During trusted CA import, the size of the imported file was more than the maximum supported	Oct 9 11:03:52:W: TRUSTED CERT IMPORT: Certificate file size is larger than supported 4096 bytes
There is a maximum of 3 trusted certificates that can be imported. If user imports a 4th one a slot full audit log will be filed	Oct 9 11:03:52:W: TRUSTED CERT IMPORT: Certificate slot is full. Import failed
The certificate index of the 3 supported certificate indexes can be only 0,1 and 2. If for some reason the index is more than this an audit log will be filed.	Oct 9 11:03:52:W: TRUSTED CERT IMPORT: Certificate index is invalid. Import failed
The certificate length of the imported certificate was found to be 0.	Oct 9 11:03:52:W: TRUSTED CERT IMPORT: Certificate length is invalid. Import failed
The certificate data imported is encoded in Base64-content-transfer encoding. If decoding this data fails audit log will be filed for decode error	Oct 9 11:03:52:W: TRUSTED CERT IMPORT: Certificate decoding failed
If certificate does not have valid fields, parse error will be filed in the audit log	Oct 9 11:03:52:W: TRUSTED CERT IMPORT: Certificate parsing failed

Other Entries

Operation	Log Details
When banner motd is configured.	Mar 27 2019 04:41:30 c System:Banner MOTD created successfully
When banner incoming is configured.	Mar 27 2019 04:42:10 c System:Banner Incoming created successfully
When banner exec is configured.	Mar 27 2019 04:41:51 c System:Banner EXEC created successfully
When banner require-enter-key is configured.	Mar 27 2019 04:41:19 c System:Bannermotd require-enter-key created successfully
When banner motd is unconfigured.	Mar 27 2019 04:43:00 c System:Banner MOTD deleted successfully
When banner incoming is unconfigured.	Mar 27 2019 04:43:13 c System:Banner incoming deleted successfully
When banner exec is unconfigured.	Mar 27 2019 04:43:26 cpaneers System:Banner EXEC deleted successfully
When banner require-enter-key is unconfigured.	Mar 27 2019 04:42:48 c System:Bannermotd require-enter-key deleted successfully
fips enable	Mar 27 2019 04:43:26 System: fips enabled successfully
Console logout	Jun 8 00:29:07 cer2024 Security: console logout by admin from USER EXEC mode
Console timeout	Jun 4 00:34:18 cer2024 Security: console timed out by admin from USER EXEC mode
Console Login Failure	May 1 12:46:56 cer2024 Security: Console access by admin rejected, 1 attempt(s) Operation
Console Login Success	Jun 7 14:40:19 cer2024 Security: console login by admin to PRIVILEGED EXEC mode
Wrong password	Jun 13 17:20:05 cer2024 Security: Wrong password attempt from 172.16.16.254 IP
Account lockout	Jun 19 17:24:53 mlxe Security: User admin is disabled due to too many login attempts
Account enabled	Jun 19 17:24:53 mlxe Security: User admin is enabled
Reset password	Jun 19 18:13:52 mlxe Security: user testuser modified by admin from console session
Manually change time	Nov 11 11:11:11 mlxe Security: System clock changed from "May 20 2019 17:42:18" to "Nov 11 2000 11:11:11"
Single command Manifest upgrade started.	Jun 7 23:39:35 mlxe Single-command upgrade started.
FIPS verification of images successful.	Jun 8 00:35:40 mlxe FIPS: Image verification passed for monitor. Jun 8 00:35:43 mlxe FIPS: Image verification passed for lp-monitor-0 Jun 8 00:36:56 mlxe FIPS: Image verification passed for primary Jun 8 00:38:00 mlxe FIPS: Image verification passed for lp-primary-0 Jun 8 00:39:50 mlxe Single-command upgrade completed successfully

Operation	Log Details
FIPS verification of images failed.	Jun 7 14:48:41 cer2024 FIPS: Image verification failed for monitor-temp Jun 7 14:50:13 cer2024 FIPS: Image verification failed for primary-temp Jun 7 14:50:19 cer2024 FIPS: Image verification failed for pbifmetro.exe Jun 7 14:50:19 cer2024 Single-command upgrade completed with error(s)
Configure audit behavior.	May 22 21:03:45 cer2024 System: Syslog server 172.16.16.254 added by admin from ssh session
RADIUS service successful connection.	May 28 21:07:12 cer2024: Radius service for Authentication session gave response=ACCEPT from server_ip=172.16.16.254
TACACS+ service successful connection.	Jun 3 23:25:34 cer2024: Tacplus service for Authentication session gave response=ACCEPT from server_ip=172.16.16.254

Appendix B - Self-Test Messages

Self-Test Message from the Console

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

```
Starting FIPS_selftest!

Running DRBG self test ...successful!
Running X931 self test ...successful!
Running SHA1 self test ...successful!
Running HMAC self test ...successful!
Running CMAC self test ...successful!
Running AES self test ...successful!
Running AESCCM self test ...successful!
Running AESGCM self test ...successful!
Running AES XTS self test ...successful!
Running DES self test ...successful!
Running RSA self test ...successful!
Running ECDSA self test ...successful!
Running DSA self test ...successful!
Running ECDH self test ...successful!
Running AES KAT test ...successful!
Running DSA KAT test ...successful!
Running HASH KAT test ...successful!
Running HMAC KAT test ...successful!
Running RSA KAT test ...successful!
Running SSH KAT test ...successful!
Running TLS KAT test ...successful!
Running TLS v1.2 KAT test ...successful!
Running SNMP KAT test ...successful!
Running 3DES KAT test ...successful!
Running CMAC KAT test ...successful!
Running ECDSA KAT test ...successful!
Running KBKDF KAT test ...secret_key_length 16
message_length 48
successful!
Running KW KAT test ...successful!
Fips crypto drbg health check tests ran successful.
FIPS Power On Self Tests and KAT tests successful.
Running FIPS Software/Firmware Integrity Test ...Verifying MP Image file
primary.....Verified OK
FIPS: Image verification passed for primary
PASSED
Verifying MP Monitor.....Verified OK
FIPS: Image verification passed for monitor
PASSED
FIPS Software/Firmware Integrity Test PASSED
```

```
Crypto module initialization and Known Answer Test (KAT) Passed
```

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

```
system memory:  2147483648,  available   1869942784
Jun  8 00:01:54.193 WcWebClientInit, kWcTcpBufferSize = 1425, kWcWorkBufferLength = 1425
Start init runconfig from start config
Load config data from flash memory...

 Fips force failure rsa test encrypt/decrypt failed as expected!

NetIron CE 2000 Boot Code Version 6.2.0
Enter 'a' to stop at memory test
Enter 'b' to stop at boot monitor
BOOT INFO: load monitor from code flash, cksum = d5b7
BOOT INFO: verify flash files -
max_code_flash_blocks[254].....................................................
BOOT INFO: debug enabled!!!
```

Appendix C - Configuring an external Syslog Server with TLS support

External Syslog server overview

The information available in this section is a representative configuration example of the many types of Syslog servers available. This section is useful for configuring a remote Syslog server and is not applicable for NetIron configuration.

Note
This is optional and for informational use only, not mandated by common criteria.

Though there are many types of Syslog servers available, the following setup procedure describes how to set up an encrypted Syslog server running on Ubuntu 10.4. The setup procedure for an encrypted Syslog server on other Linux operating systems such as Red Hat or Centos is simiilar except for the differences in commands.

You must set up stunnel as a server and a client on your server. As a server, stunnel listens on port 60516 to connections from its client peers, and all connections are forwarded to the locally-running rsyslog listening at port 61514. As a client, rsyslog forwards messages to the stunnel local portal at port 61514, and stunnel local port forwards data by way of the network to port 60514 to its remote peer.

Setting up stunnel

Procedure

1. Install the stunnel utility with the following command:

```
$ sudo apt-get install stunnel4
```

2. Edit the file with the `/etc/default/stunnel4` path to start the service on system startup. Use a text editor such as vi.

```
$ sudo vi /etc/default/stunnel4
```

3. Change the line `Enabled=0` to `Enabled=1`.

Creating a certificate with the OpenSSL toolkit

Procedure

1. Enter the following command:

```
cd /etc/stunnel
```

2. To create the `/etc/stunnel/stunnel.pem` file with a certificate and key for SSL, enter the following command

```
$openssl req -new -x509 -days 365 -nodes -out stunnel.pem -keyout
/etc/stunnel/stunnel.pem
```

3. To change the permissions for the certificate that you generated, enter the following command.

```
$ sudo chmod 600 /etc/stunnel/stunnel.pem
```

Creating a configuration file

Procedure

1. Enter the following command to open the stunnel.conf file:

```
$sudo vi /etc/stunnel/stunnel.conf
```

2. Comment out the features that you do not require, such as the [pop3s], [ssmtp], and [imaps] sections.
3. Change the `cert=/etc/stunnel/mail.pem` line to `cert=/etc/stunnel/stunnel.pem`.
4. Add the following lines and save the file.

```
; Certificate/key is needed in server mode
cert = /etc/stunnel/stunnel.pem
key = /etc/stunnel/stunnel.pem

; Some debugging stuff useful for troubleshooting
debug = 7
foreground=yes

[ssyslog]
accept = 60514
connect = 61514
```

Changing the stunnel4 startup file

About This Task

Enter the `cd /etc/init.d/stunnel4` command and change `ENABLED=0` to `ENABLED=1`.

Restarting the stunnel service

To restart the stunnel service, enter the following command.

About This Task

```
$sudo /etc/init.d/stunnel4 restart
```

Configuring rsyslog

Ubuntu 10.04.3 comes with rsyslog 4.2.0 as its default logger. You can add MySQL output support and the Reliable Event Logging Protocol (RELP). Enter the following command:

About This Task

```
root@linux:~$sudo apt-get install rsyslog-mysql rsyslog-relp
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
        dbconfig-common librelp0
The following NEW packages will be installed:
        dbconfig-common librelp0 rsyslog-mysql rsyslog-relp
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 677kB of archives.
After this operation, 2,335kB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

During the installation process, complete the following steps:

Procedure

1. Create the tables that are needed in MySQL when prompted.
2. Set the MySQL root password.
3. Create a password that the rsyslog processes will use in the configuration files.

Enabling accepting remote logs

To turn on accepting remote logs, edit the `/etc/rsyslog.conf` file by commenting out the following lines:

About This Task

```
# provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 61514
```

Restarting rsyslog service

To restart the rsyslog service, enter the following command:

About This Task

```
root@linux:~$sudo service rsyslog restart
```

Note

Extreme recommends rebooting the Linux server after the setup.

Printing log messages

Enter the following command to update the log-watcher window with logged messages as they arrive:

About This Task

```
root@linux:~$tail -f /var/log/messages
```

You can also configure a web user interface to display the syslog messages using the Reliable Event Logging Protocol (RELP). Refer to http://www.linuxjournal.com/content/centralized-logging-web-interface for more information.

Requirements for valid trusted certificates used with TLS applications

Certificates (both server and trusted) must meet the following criteria.

Before You Begin

- Only RSA certificates are accepted.
- The public key must be greater than or equal to 2048 bits.
- The Signature Algorithm must be using SHA256.
- The device being a Syslog client, it needs to have the Syslog server's Root CA certificate installed on it before the TLS connection is attempted.
- An expired certificate is not accepted.
- A certificate with an empty Subject Alternative Name (SAN) field and invalid Common Name (CN) is rejected.

  1. For SAN, check for the matching incoming server IPv4 address.
  2. IF SAN doesn't match, then CN is validated for incoming server IPv4 address.
- Upto 3 length of chain certificate is supported. Self-signed certificate is no longer supported in this mode.
- The TLS connection must use the approved cipher suites.

Appendix D - Radius Server with TLS Support

Configuring FreeRADIUS with TLS support on page 55

Configuring FreeRADIUS with TLS support

The FreeRADIUS server comes with native support of TLS and it can also be used with stunnel proxy which relays TCP packets to FreeRADIUS. Refer for stunnel specific configuration.

[radius] accept = 61514 connect = 1812

61514 is the SSL port configured on device. The FreeRADIUS server has a sites-available directory in which the file **inner-tunnel** has configuration, which represents the client with incoming requests. When using stunnel as a proxy server, with FreeRADIUS running on the same machine, inner-tunnel configuration is as following.

```
 [root@rhel-105-201 sites-available]# vim inner-tunnel
listen {
 ipaddr = 127.0.0.1
 proto = tcp
 port = 1812
 type = auth+acct
}
```

The IP address is the local loopback since FreeRADIUS and stunnel processes run on the same machine and FreeRADIUS recieves the relayed requests from stunnel. The IP address on the device is considered, when stunnel is running on that specific device. When using FreeRADIUS server with direct TLS support the inner-tunnel have following configuration.

```
server inner-tunnel {
 listen {
 ipaddr = 10.24.12.65
 port = 2083
 type = auth+acct
 proto = tcp
 tls {
 private_key_file = /root/tmanicka/NI/radius/rsakey2048.pem
 certificate_file = /root/tmanicka/NI/radius/rsacert2048_days1095_sha256_SAN.pem
 ca_file = /root/tmanicka/NI/radius/rsacert2048_days1095_sha256_SAN.pem
 }
 }
```

The IP address is the management IP of the device, port is the TLS port configured on device.

When using stunnel proxy the certificates and private key are imported in **stunnel.conf** as stunnel is the TLS server. But when using direct TLS with FreeRADIUS, the certificates and private key is imported via the inner tunnel file.

Note
All certificate chain validation process and certificate related parameters remain the same as in Syslog over TLS.

The FreeRADIUS server contains a file **client.conf** which is updated with the client IP address and the same shared secret configured on device. When using stunnel as proxy the **client.conf** should have an entry as following.

```
client localhost{
ipaddr = 127.0.0.1
secret = Pass@123
proto = tcp
require_message_authenticator = no
nastype = "other"
}
```

The name of the entry namespace is not important, but the *ipaddr*, *secret* and *proto* must be correct. The *ipaddr* is the local loopback or the machine IP hosting stunnel, *secret* is the shared secret configured on device, and *proto* must be TCP as the default protocol for RADIUS is UDP.

When using native TLS support in FreeRADIUS the **client.conf** is as following.

```
client radsec{
ipaddr = 10.24.12.65
secret = Pass@123
proto = tcp
require_message_authenticator = no
nastype = "other"
}
```

Note
When using stunnel proxy and direct TLS with RADIUS the *ipaddr* can be generically assigned to character " *" .

Related Topics

Encrypted Syslog servers in Common Criteria mode on page 33

NetIron devices in any mode send the generated Syslog messages in real time to the local log storage on the device and to a Syslog server (only if a Syslog server is configured and available).