Extreme Fabric Engine Common Criteria Configuration Guide 9.1.100

Supporting Series 7720, 7520, 5720, 5520, 5420, 5320

May 2026

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: https://www.extremenetworks.com/about-extreme-networks/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/

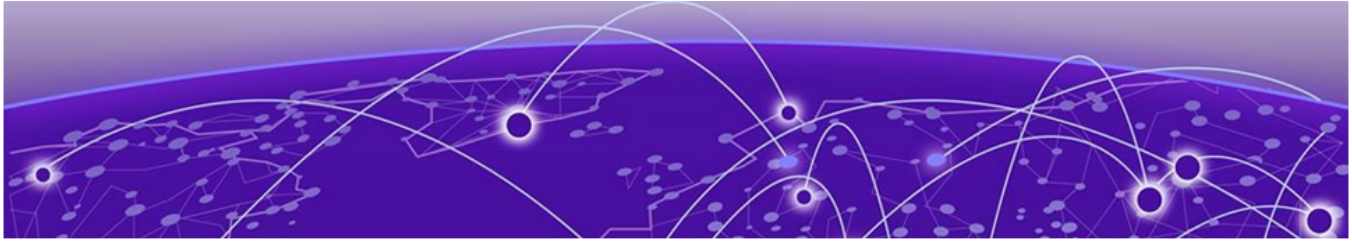


Table of Contents

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 Extreme Networks switches, the product is referred to as *the switch*.

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 articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

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 2800. 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 User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

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

To send feedback, email us at Product-Documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.

Common Criteria Certification Configuration

Overview

Common Criteria certification for a device enforces a set of security standards, and limits features to comply with Common Criteria standards. The topics in this section guide you through the process of configuring your system to comply with Common Criteria standards.

When administrators log in with role-based credentials, their access is limited to commands they have privileges and permissions to use, based on Common Criteria standards.

Note
The term *administrator* is used interchangeably in this document with *security administrator* in the Security Target.

Additionally, network management communication paths are protected against modification and disclosure using SSHv2, TLS, and HTTPS. The audit channel to an external syslog server is protected using TLS encapsulation.

The communication channel between the Fabric Engine™ device and RADIUS authentication servers should be protected by TLS encapsulation.

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

Common Criteria compliance mode supports devices running Fabric Engine™ version 9.1.100. Cryptographic Algorithm Validation System (CAVS) certifies all cryptographic algorithms required by and used in Common Criteria.

Evaluated Devices

The following switches, running Fabric Engine™ version 9.1, were evaluated for compliance.

- 7720 Series
- 7520 Series
- 5720 Series
- 5520 Series
- 5420 Series
- 5320 Series

Supported Cryptographic Methods

In the evaluated configuration, the sets of supported ciphers and key exchange methods cannot be changed.

TLS

TLS The switch supports TLS 1.2 as defined in RFC 5246. For more information, see Enable a TLS Connection to the Syslog Server.

Note
TLS 1.0 and TLS 1.1 are not supported.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

The switch performs the TLS key exchange with the following ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) curves.

- secp256r1
- secp384r1
- secp521r1

SSH

The switch supports only Secure Shell version 2 (SSHv2). For more information, see Secure Shell Configuration. The following encryption algorithms are supported.

- AES-128-CBC
- AES-256-CBC
- AES-128-CTR
- AES-256-CTR
- aes128-gcm@openssh.com or aes256-gcm@openssh.com

The following MAC ciphers are supported for SSH.

- HMAC-SHA-1
- HMAC-SHA2-256

The switch performs the SSH key exchange with the the following methods:

- Diffie-Hellman-Group14-SHA256
- Diffie-Hellman-Group16-SHA512
- Diffie-Hellman-Group18-SHA5126

The switch supports only Secure Shell version 2 (SSHv2). For more information, see Secure Shell Configuration on page 23.

Initial Switch Configuration Tasks

An administrator sets up the Extreme Portal switch for an evaluated configuration with the following tasks.

Access to the Switch

A Fabric Engine device can be accessed or managed using various options. These include console access (over serial interface), SSH, RESTCONF requests, and NETCONF requests.

Note
RESTCONF and NETCONF are not covered in this evaluation.

The serial connection is described in Establish a Serial Connection on page 13.

You can use the following methods to the following instructions to access the switch.

Access the device using SSH from a remote client:

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

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

Serial Connection

The serial connection is described in Establish a Serial Connection on page 13.

SSH

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

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

Access the device using SSH from a remote client:

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

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

HTTPS

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

Establish a Serial Connection

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

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

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

1. Configure the terminal protocol as follows.
   115200 baud rate
   8 data bits
   1 stop bit
   No parity
   No flow control
2. Connect the RJ-45 or USB cable to the console port on the device.
3. Connect the other end of the cable to the terminal or computer serial port.
4. Turn on the terminal.
5. Provide the first-time administrative credentials to gain access to the switch.
   The following is an example of an administrator's first-time log-in to the switch.

```
Login: admin
Password: *****
```

```
        This is an initial attempt using the default username and password.
        Please change the username and password to continue.

Enter the new name : aminuser
Enter the New password : ***************
Re-enter the New password : ****************

Password changed successfully

        User is logged in for the first time
00000000 GlobalRouter SW INFO Password modified for user aminuser
```

6. To close a serial connection, run the **exit** or **logout** command.

Initial System Log-in and Credential Change

The administrator initially logs on to the switch using the default user name of `rwa` and the default password of `rwa` . The switch then prompts the administrator to create a new user name and password. The following is an example of an administrator's first log-in to the switch.

```
Login: admin
Password: *****


        This is an initial attempt using the default username and password.
        Please change the username and password to continue.

Enter the new name : adminuser
Enter the New password : ***************
Re-enter the New password : ****************

Password changed successfully

        User is logged in for the first time
00000000 GlobalRouter SW INFO Password modified for user aminuser
```

Configure the Out-of-Band Management Interface

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

Segmented Management is a means of managing devices in which the management plane (management protocols) is separate from the control plane (routing plane) from a process and data-path perspective. You use the out-of-band method for Common Criteria configuration. For more information, see the *Fabric Engine™ User Guide* for version 9.1 or later.

Note
The OOB Segmented Management Instance is not supported on 5320 Series supports In-Band management only. See Configure the In-Band Management Interface for more information.

1. Access out-of-band configuration mode.

```
# enable
# configure terminal
(config)# mgmt oob
```

2. Configure the IP address and mask for the management port.

```
# ip addr <ip-addr/mask>
```

3. Configure IP routes for the management network.

```
# ip route <ip-addr/mask> next-hop <ip-addr> weight 300
```

4. Verify the management IP interface information.

```
# show mgmt topology-ip
```

Configure Boot Flags

The Extreme Portal operating system has several flags that control certain services during system boot. The following table describes the flags that have a Common Criteria (CC) requirement.

Table 4: Common Criteria boot flags

Flag	Description	Default	CC Requirement	Command
block-snmp	Activate or disable SNMP	disabled	disabled	`no boot config flags block-snmp`
ftpd	Activate or disable FTP server	disabled	disabled	`no boot config flags ftpd`
hsecure	Activate or disable high secure mode	disabled	disabled	`no boot config flags hsecure`
sshd	Activate or disable the SSH server	disabled	enabled	`boot config flags sshd`
tftpd	Activate of disable the TFTP server	disabled	disabled	`no boot config flags tftpd`
telnetd	Activate or disable the Telnet server	disabled	disabled	`no boot config flags telnetd`

1. Access out-of-band configuration mode.

```
# enable
# configure terminal
# mgmt oob
```

2. Display the current boot flags.

```
# show boot config flags
```

The command returns a list of flags and the setting (true or false) for each.

Enhanced Secure Mode

Enhanced secure mode enables role-based authentication (RBAC) and stronger password complexity, length, and minimum change intervals.

Role-Based Access

When you enable enhanced secure mode (see Enable Enhanced Secure Mode on page 17), the device supports RBAC and the following access levels for local authentication, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System Plus (TACACS+) authentication.

Table 5: RBAC levels

Access Level	Description	Log-in Location
Administrator	This access level allows all read-write access, and can change security settings. This level can configure CLI and web-based management user names, passwords, and SNMP community strings, and can view audit logs.	SSH, Telnet, or console
Privilege	This access level has the same access permission as the administrator, but cannot use RADIUS or TACACS+ authentication. The system must authenticate this access level within the device at the console level. This access level is also known as *emergency-admin*.	Console
Operator	This access level can view most device configuration and status information, but cannot access audit logs or security settings. This access level can change physical port settings at Layer 2 and Layer 3.	SSH, Telnet (in-band or management), or console
Auditor	This access level can view configuration information, status information, and audit logs.	SSH, Telnet (in-band or management), or console
Security	This access level can change only security settings, and can view configuration and status information.	SSH, Telnet (in-band or management), or console

Each user name is associated with a certain role in the product, with the authorization rights for viewing and running commands that are available for that role. With enhanced secure mode enabled, the person with the access level of administrator configures the default log-in and password values for the other users, based on their access levels.

Password Complexity

Password requirements in enhanced secure mode are strict by default.

- Passwords require the following characters: 2 upper case, 2 lower case, 2 numerical, and 2 special (!, @, #, $, %, ^, *, (,), and &).
- The minimum password length can be from 8 to 32 characters. The default is 15.
- The minimum number of consecutive failed log-in attempts that can occur before a user is locked out can be from 1 to 255 attempts. The default is 3.

You can configure the minimum password length and the number of failed password attempts before lockout. For more information, see Configure Global Password Settings and Enable a Locked-Out User Account.

Enable Enhanced Secure Mode

In a Common Criteria configuration, you must enable enhanced secure mode in non-JITC sub-mode, which is more restrictive and prevents the use of some CLI commands that are commonly used for troubleshooting.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Enable enhanced secure mode.

```
(config)# boot config flags enhancedsecure-mode non-jitc
```

3. Save the configuration.

```
(config)# save config
```

4. Restart the device.

```
(config)# boot config /intflash/<config-file-name> -y
```

Create User Accounts

With enhanced secure mode enabled, the person with the role of administrator configures the user accounts for the other users and assigns the appropriate role. For more information about user roles, see Enhanced Secure Mode.

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Create an account with the appropriate role.

```
(config)# password create-user {auditor|operator|privilege|security} <username>
```

3. Save the configuration.

```
(config)# save config
```

The following is an example of creating an account for user bakers with the role of operator.

```
# enable
# configure terminal
```

```
(config)# password create-user operator bakers
(config)# save config
```

Configure User Passwords

With enhanced secure mode enabled, the person with the role of administrator creates and changes the passwords for the other users. For more information about password requirements, see Enhanced Secure Mode on page 15.

1. Enter global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Create or change a password.

   ```
   (config)# password set-password user-name <user-name>
   ```

3. Enter the password.

4. Save the configuration.

   ```
   (config)# save config
   ```

The following is an example of assigning a password for user bakers.

```
# password set-password user-name bakers
Enter the Old password : **********
Enter the New password : **********
Re-enter the New password : **********
00000000 GlobalRouter SW INFO Password modified for user bakers
```

Configure Global Password Settings

You can configure the minimum password length and the length of time an account is locked after the maximum number of log-in failures occurs. By default, a user is locked out after three consecutive failed log-in attempts

1. View the current password policy before making any changes.

   ```
   # show cli password
   ```

2. Access global configuration mode.

   ```
   # enable
   # configure terminal
   ```

3. Set the minimum password length to at least 15 characters for all users.

   ```
   (config)# password min-passwd-len <value>
   ```

   The maximum allowable number of characters is 20.

4. Configure the number of seconds that an account is to remain locked after three consecutive failed log-in attempts.

   ```
   (config)# password default-lockout-time <value>
   ```

   The default is 60 seconds. Acceptable values range from 60 to 65000.

5. Save the configuration.

   ```
   (config)# save config
   ```

Enable a Locked-Out User Account

Only the user with the Privilege role can enable a locked-out user account. This role has access to the system only through the serial console.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Enable the locked-out account.

```
(config)# password enable-user user-name <user-name>
```

3. Save the configuration.

```
(config)# save config
```

Set the System Date, Time, and Time Zone

You can manually configure the date, time, and time zone. You can also synchronize a device with an external Network Time Protocol (NTP) server. For more information, see Appendix: Network Time Protocol.

1. Log in to the device to access user EXEC mode.
2. Configure the date and time in the following format: month, day, year, hour, minutes, seconds.

```
# clock set <MMddyyyyhhmmss>
```

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

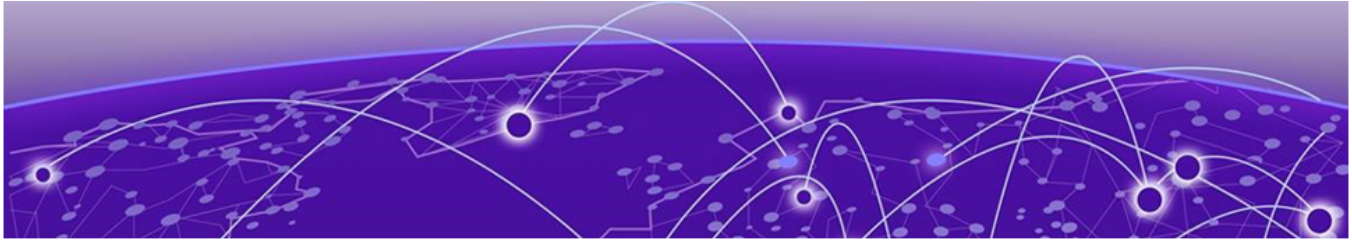
```
# clock time-zone <time-zone-name> <sub-area> <secondary-sub-area>
```

The following example configures the time zone for the area of Vevay in Indiana, America.

```
# clock time-zone America Indiana Vevay
```

Tip

You can run the **`clock time-zone`** command without parameters to see the options for time zone names, sub-areas, and secondary sub-areas.



Network Time Protocol

Overview

Network Time Protocol (NTP) synchronizes the internal clocks on devices across a network with a coordinated Universal Time Clock (UTC), the primary time standard by which the world regulates clocks and time. UTC is used by devices that rely on having a highly accurate, universally accepted time, and can synchronize computer clock times to a fraction of a millisecond. NTP uses a hierarchical, semi-layered system of levels of clock sources called a stratum. Each stratum is assigned a layer number starting with 0 (zero), with 0 meaning the least amount of delay. The layer number defines the distance, or number of NTP hops away, from the reference clock. The lower the number, the closer the device is to the reference clock.

Fabric Engine version 9.1.100 uses NTPv4.

For complete information about NTP as it relates to Fabric Engine, see the *Fabric Engine User Guide 9.1.0*.

Limitations and Requirements

The Fabric Engine switch acts as the NTP client. Use of the switch as an NTP server is not supported for Common Criteria.

- The Fabric Engine switch acts as the NTP client. Use of the switch as an NTP server is not supported for Common Criteria.
- The administrator must use NTP authentication with SHA1 authentication. For more information, see Manage NTP Authentication.
- NTP multicast and broadcast packets are not supported.

Specify and Enable the NTP Server

You can specify the IPv4 or IPv6 address of the NTP server and then verify that the action was successful. The Fabric Engine switch, which acts as the NTP client, queries the NTP server for time information. For NTPv4, you can configure a maximum of 10 IPv4 NTP servers and 10 IPv6 NTP servers.

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Specify and enable the NTP server.

```
(config)# ntp server <ip-addr> enable
```

3. Verify that the server was added.

```
(config)# show ntp server
```

Manage NTP Authentication

You can ensure that the switch obtains its time only from an authenticated, known source (the NTP server). The switch uses the Secure Hash Algorithm 1 (SHA1) algorithm for authentication, matching the authentication key on the NTP server with the authentication key on the NTP client (the Switch Engine switch). You must configure an authentication key for each NTP server, up to 10.

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Create a SHA-1 key ID and a secret key.

```
(config)# ntp authentication-key <keyid> type sha1
Enter the NTP secret key : **********
Re-enter the NTP secret key : **********
```

   Valid values for the key ID range from 1 to 65534 characters. Valid values for the secret range from 0 to 20 characters.

3. Enable SHA1 authentication on the NTP server.

```
(config)# ntp server <ip-addr> auth-enable
```

   Use the IPv4 or IPv6 IP address of the NTP server.

4. Assign an authentication key to the NTP server.

```
(config)# ntp server
```

   Use the IPv4 or IPv6 IP address of the NTP server and the key ID you created in step 2.

5. Confirm the authentication key.

```
(config)# show ntp key
```

Configure the NTP Update Interval

Fabric Engine switches specify the time interval between successive NTP updates as a power of 2 in seconds. The default interval is 2 to the power of 8 seconds.

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. (Optional) Configure the update interval.

```
(config)# ntp interval <interval>
```

Valid <interval> values range from 4 through 17.

Restrict NTP Traffic

With the `ntp-restrict` command capability, you identify the IPv4 or IPv6 addresses from which NTP traffic is allowed. Traffic from all other addresses is ignored.

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Restrict an IP address.

```
(config)# ntp restrict <ip-addr>
```

3. Repeat step 2 as many times as needed, for up to 128 IP addresses.

```
Verify the restricted addresses.
```

4. Verify the restricted addresses.

```
(config)# show ntp restrict
```

Display NTP Status Information

You can use various `show` commands to display information such as the global NTP status and NTP key information. The following examples show typical output for the commands. Your output will vary.

1. Display the global NTP status.

```
# show ntp
********************************************************************************
Command Execution Time: Wed Sep 28 14:35:01 2022 GMT
********************************************************************************
NTP Master
================================================================================
Version Enabled Stratum
--------------------------------------------------------------------------------
4 False 1
================================================================================
NTP Client
================================================================================
Version Enabled Interval Last Update Time Synchronized
To
--------------------------------------------------------------------------------
4 True 8 Wed Sep 28 14:33:24 2022 GMT 192.0.2.0 (Stratum:3)
```

2. Display NTP authentication key information.

```
# show ntp key
Key Index Trusted Auth Key String (encrypted)
=============================================================
200 Yes SHA-1 23:24:6c:35:4a:35:79:74:65
```

3. Display restricted IP addresses.

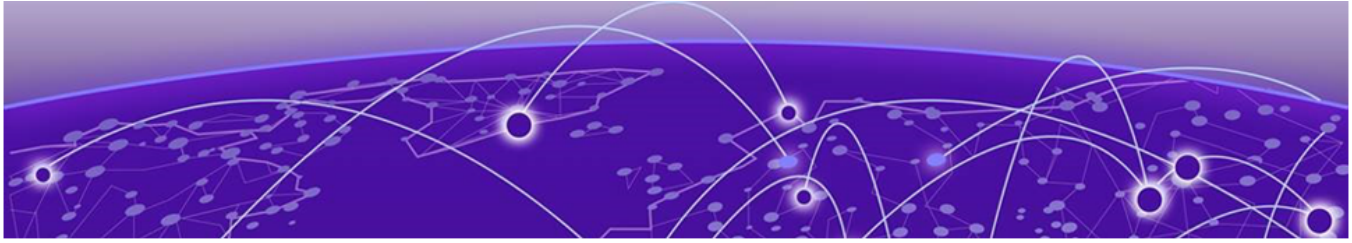
```
# show ntp restrict
====================================
NTP Restrict Information
====================================
TYPE ADDRESS MASK/PREFIX LEN
IPv4 x.x.x.x 23
```

4. Display NTP server information.

```
# show ntp server
*********************************************************************
Command Execution Time: Wed Sep 28 14:35:17 2022 GMT
*********************************************************************
NTP Server
=====================================================================
Server IP Enabled Auth Key Id Auth Type
---------------------------------------------------------------------
192.0.2.0 true false 0 N/A
```

5. Display NTP statistics.

```
# show ntp statistics
*********************************************************************
Command Execution Time: Wed Sep 28 14:35:21 2022 GMT
*********************************************************************
NTP Server : 10.3.33.244
----------------------------------------
Stratum : 3
Version : NTPv4
Broadcast : No
Auth Enabled : Disabled
Auth Status : Not-Auth
Sync Status : System Peer
Reachability : Reachable
Root Delay : 0.000
Root Disp : 11.719
Delay : 0.620
Dispersion : 12.129
Offset : -0.209
Precision : -23
Jitter : 0.043
Last Event : Popcorn
```



Connectivity

Overview

Ensure that your devices can communicate and allow data transfer and resource sharing in compliance with Common Criteria standards for security and stability.

Configure the Domain Name System

Use this task to configure the DNS for Common Criteria compliance.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Configure the host name for the device.

   The value of the SNMP *sysName* variable is the prompt that an administrator sees when logging into the device. The *sysName* becomes the host name of the device.

```
(config)# snmp-server name <sysName>
```

3. Configure the domain name.

```
(config)# ip domain-name <domain-name>
```

4. Configure the external DNS server.

```
(config)# ip name-server {primary|secondary|tertiary} <ip-addr>
```

5. Verify the DNS configuration.

```
(config)# show ip dns
```

6. Verify the DNS resolution by pinging the DNS server.

   The following shows three examples, one for a DNS host name, one for an IPv4 address, and one for an IPv6 address.

```
(config)# ping <host-name>
(config)# ping <ipv4-addr>
(config)# ping <ipv6-addr>
```

Secure Shell Configuration

Secure Shell (SSH) is a client and server protocol that specifies the way to conduct secure communications over a network.

SSH supports a public and private key encryption scheme. Using the public key of the host server, the client and server (the Switch Engine switch) negotiate to generate a session key known only to the client and the server. This one-time key encrypts all traffic between the client and the server.

The switch supports only SSH version 2 (SSHv2). The evaluated configuration has the following SSH requirements, which can be managed by an administrator.

Encryption algorithms

Only the following algorithms, which are enabled by default, are approved for use in the Common Criteria configuration. You can use some or all of these algorithms.

- AEAD-AES-128-GCM-SSH
- AEAD-AES-256-GCM-SSH
- AES-128-CBC
- AES-256-CBC
- AES-128-CTR
- AES-256-CTR
- AES 128-gcm@openssh.com
- AES256-gcm@openssh.com

MAC algorithms

Only HMAC-SHA2-256, AEAD-AES-128-GCM-SSH, AEAD-AES-256-GCM-SSH, and implicit algorithms are approved and enabled by default.

Key exchange methods

The switch performs the SSH key exchange with the the following methods:

- Diffie-Hellman-Group14-SHA256
- Diffie-Hellman-Group16-SHA512
- Diffie-Hellman-Group18-SHA5126

User authentication methods

Public key and password methods are supported, as is authentication by X.509 digital certificates. Password authentication is enabled by default. For more information, see Enable Public Key Authentication, Enable X.509 Authentication, and Certificate Management.

Host authentication methods

The RSA method is supported, as is authentication by X.509 digital certificate. For more information, see Enable RSA Authentication and Generate the Host Key, Enable X.509 Authentication, and Certificate Management.

Session limitations

The same session keys can be used for no more than 1 hour and with no more than 1 gigabyte of transmitted data. If either of these thresholds is exceeded, rekeying is required. For more information, see Configure the SSH Rekeying Interval on page 28.

Packet limitations

Packets in excess of 32,768 bytes are dropped. Packets of 32,769 bytes and more are considered oversized.

Enable SSHv2

You must enable the SSH service on the switch before you can connect to the switch from an external SSHv2 client. This procedure does not stop or start the SSH service. It merely enables the service in Fabric Engine .

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Enable SSHv2 on the switch.

```
(config)# boot config flags sshd
```

3. Save the changes to the configuration file.

```
(config)# save config
```

Disable `DSA Auth`

DSA (Digital Signature Algorithm) authentication is a weak, leakage-prone algorithm that is enabled by default. Disable it to conform to Common Criteria Configuration requirements. Perform this procedure from the console.

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Disable `dsa-auth` and save the configuration.

```
(config)# no ssh dsa-auth
# save config
```

Enable RSA Authentication and Generate the Host Key

RSA host keys are used to authenticate connections between the device and clients on remote systems. RSA authentication uses SHA-1, SHA-256, and SHA-512 hashing algorithms as part of the SSHv2 (secure shell) protocol.

Perform this procedure from the console.

1. View the current SSH server configuration before making changes.

```
# show ssh global
```

2. Access global configuration mode.

```
# enable
# configure terminal
```

3. Disable the `iqagent` application

   The application must be disabled before you can disable SSH in the next step.

```
(config)# application
(config-app)# no iqagent enable
(config-app)# exit
```

4. Disable SSH and enable RSA authentication.

```
(config) no ssh
(config)# ssh rsa-auth
```

5. Generate the host key.

```
(config)# ssh rsa-host-key <key-size>
```

   Valid values for the size of the host key range from 512 to 2048. The default is 2048.

   Caution
   Configuring the size of the host key for less than 2048 will take the TOE out of the evaluated configuration.

6. Re-enable SSH and save the configuration.

```
(config)# ssh
(config)# end
# save config
```

Enable Public Key Authentication

An SSH key pair is two cryptographically secure keys (one public key and one private key) that can be used to authenticate a client to an SSH server. The private key is retained by the client and must be kept absolutely secret. Any compromise of the private key can enable an attacker to log into servers that are configured with the associated public key without additional authentication. The associated public key can be shared freely without negative consequences. The public key can be used to encrypt messages that *only* the private key can decrypt. This property is employed as a way of authenticating with the key pair.

Note
Ensure that you can access the public key from the client system.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Use SCP to transfer the public key from the client system to the Fabric Engine system.

3. Rename the public key to correspond with the user role it will be used for.

   Administrator: rsa_key_admin
   Operator: rsa_key_operator
   Auditor: rsa_key_auditor
   Security: rsa_key_security

```
# copy /intflash/shared/id_rsa.pub /intflash/shared/rsa_key_admin
# copy /intflash/shared/id_rsa.pub /intflash/shared/rsa_key_operator
# copy /intflash/shared/id_rsa.pub /intflash/shared/rsa_key_auditor
# copy /intflash/shared/id_rsa.pub /intflash/shared/rsa_key_security
```

4. Install the key into the SSH configuration.

   Usage for the command is `ssh install-user-key {admin, operator, auditor, security, priv} {public, private} {rsa,dsa}`. The key type must be RSA and the type of key to install is public, as shown in the following examples.

```
(config)# ssh install-user-key admin public rsa
(config)# ssh install-user-key operator public rsa
(config)# ssh install-user-key auditor public rsa
(config)# ssh install-user-key security public rsa
```

Enable X.509 Authentication

Perform this procedure from the console.

1. View the current SSH server configuration before making changes.

```
# show ssh global
```

2. Access global configuration mode.

```
# enable
# configure terminal
```

3. Disable the `iqagent` application

   The application must be disabled before you can disable SSH in the next step.

```
(config)# application
(config-app)# no iqagent enable
(config-app)# exit
```

4. Enable X.509 authentication and disable all other authentication methods.

```
(config)# no ssh
(config)# no ssh rsa-auth
(config)# no ssh dsa-auth
(config)# no ssh pass-auth
(config)# ssh x509-auth enable
```

5. Re-enable SSH and save the configuration.

```
(config)# ssh
(config)# end
# save config
```

Configure the SSH Rekeying Interval

SSH servers rekey (or force) an SSH connection between server and client after the configured interval is reached or the configured amount of data is transferred (whichever occurs first). For the evaluated configuration, the administrator must ensure

that the interval is no more than 1 hour and that the data limit is no more than 1 gigabyte. SSH must remain enabled while you configure rekeying.

Note
Ensure that the related certificates are added to the system and are ready to be used for authentication. For more information, see Certificate Management.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Enable SSH rekeying.

```
(config)# ssh rekey enable
```

3. Configure the amount of data (in GB) that triggers a rekey.

```
(config)# ssh rekey data-limit 1
```

Although valid values range from 1 to 6 gigabytes, only 1 gigabyte is supported in the evaluated configuration.

4. Configure the number of hours that triggers a rekey.

```
(config)# ssh rekey time-interval 1
```

Although valid values range from 1 to 6 hours, only 1 hour is supported in the evaluated configuration.

View SSH Status and Settings

You can view such SSH information as the number of active sessions, the version, the connection port, and authentication information.

1. Access user EXEC mode.

```
# enable
```

2. View global SSH information.

```
# show ssh global
```

3. View SSH information for the active session.

```
# show ssh session
```

TLS Negotiation

Fabric Engine supports reference identifier matching, according to RFC 6125. The reference identifier is specified during configuration of the TLS connection. Supported reference identifiers are DNS names for the Subject Alternative Name (SAN) and the Common Name (CN). As part of negotiating the TLS connection, Fabric Engine verifies that the client certificate's SAN or CN contains the expected reference identifier. The CN is checked only if the SAN is absent. Then, a connection is established only if the

client certificate is valid, trusted, has a matching reference identifier, and passes the revocation check.

Note

- If the TLS session fails because the OCSP server cannot be contacted, you are instructed to verify the network path to the OCSP server and the status of the server, and then fix any issues. When the OCSP server is not reachable, Fabric Engine accepts the certificate as 'not revoked' and continues the connection.
- If a successful TLS session is inadvertently broken, you can reestablish the session as described in Reconnect a TLS Session.

Reconnect a TLS Session

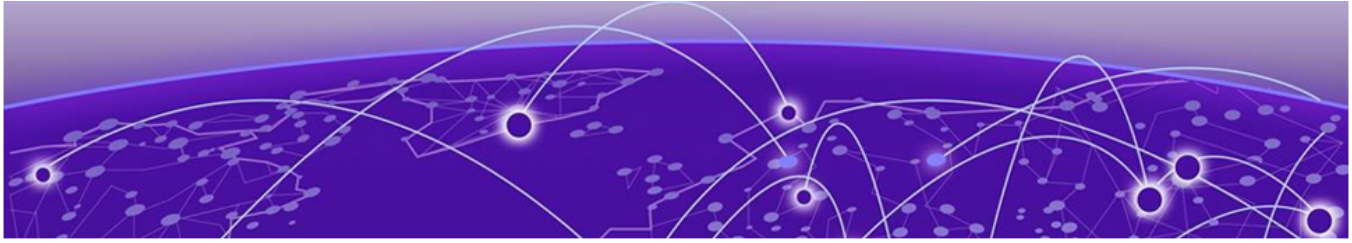
You can manually reconnect a TLS session that is inadvertently disconnected but not automatically reestablished. The system automatically attempts to reconnect a TLS session. However, if those attempts fail, for reasons such as exceeding the threshold for reconnection attempts, you can manually reconnect the session. Take the following steps to disable and then enable the syslog server in the switch, which causes the TLS session to reconnect.

1. Disable the syslog server.

```
# no syslog enable
```

2. Enable the syslog server.

```
# syslog enable
```



Certificate Management

Overview

A digital certificate is an electronic document that identifies the subject, proves the ownership of a public key, and is digitally signed by a certificate authority (CA) that certifies the validity of the information in the certificate.

A digital certificate is valid for a specific time period.

Digital certificates in the X.509 v3 format provide identity management. The switch uses PKI support to obtain and use digital certificates for secure communication in the network.

A chain of signatures by a CA and its intermediate certificate CAs binds a given public signing key to a given digital identity. Fabric Engine can authenticate SSH users with X.509 certificates and can authenticate a network service that uses TLS. The system validates X.509 v3 certificates according to RFC 5280 for the following purposes:

- As a TLS client, the system validates the certificate presented during the TLS negotiation with the syslog server.
- As an SSH server, the system validates the certificate presented by an administrative user during the establishment of an SSH-protected session offering the admin CLI.
- When certificates are loaded into the system, the imported certificates are validated.

In all of these scenarios, the X.509 certificate-validation process includes the following:

- Certificate expiration date check
- Certificate path (continuity of the certificate chain) validation up to the trusted CA
- Certificate revocation check
- Public key, key algorithm, and parameters check
- Check of certificate issuer
- Process certificate extensions

The system requires the certificate presented by the syslog server to include the `ServerAuth` EKU, and requires CA certificates to include the `BasicConstraints` flag as true. The system ignores all other EKU in certificates.

Certificates presented by an administrator to the system's SSH server must include the user identity (username@domain.com) as a `PrincipalName` in the `SubjectAltName` (SAN) extension.

Certificate Provisioning Methods

Fabric Engine switches support two methods of certificate provisioning, but only the offline method is supported for an evaluated configuration.

Offline certificate management

The offline method requires a valid administrator to manually install every certificate file into the Fabric Engine Certificate Management sub-system, including trusted root, CA, and leaf certificates. This method is the only one supported in the evaluated Common Criteria configuration.

Offline certificate management supports switches that cannot communicate with the CA to obtain the identity certificate or certificates online by certificate enrollment operation.

The CSR is used to obtain the offline identity certificate. Configure the subject and RSA key-pair to obtain the offline identity certificate. You can generate and store up to 10 RSA keys identified by the key name label. To obtain multiple offline certificates, you specify a Distinguished Subject Name and a Key Name.

You install the root CA certificate and all the intermediate CA certificates of the certificate chain in the switch before installing the offline identity or device certificate. All the intermediate and root CA certificates are stored in the certificate store and are used for CA certificate chain validation.

The CA certificate chain validation starts from the issuing CA certificate to the root CA certificate during the installation of offline identity certificate. The offline identity certificate is installed only if the CA certificate chain validation, subject, and key match.

Online certificate management

The online method requires only the trusted root CA certificate to be installed manually. This method uses the Simple Certificate Enrollment Protocol (SCEP) to obtain the certificates that the system needs.

Certificate Validation With OCSP

The Online Certificate Status Protocol (OCSP) is used to check the revocation status of X.509 v3 certificates.

The OCSP server, which is operated by the issuing CA, receives a request from the switch for the status of a certificate. The request includes the certificate serial number for validation. The OCSP server verifies the certificate status and sends a response to the switch. Based on the response, the switch validates the certificate or rejects the certificate if its status is 'revoked'.

When the OCSP server is not reachable, Fabric Engine performs the following actions:

- For TLS, Fabric Engine accepts the certificate as 'not revoked.'
- For SSH, the Fabric Engine rejects the certificate.

Digital Certificate Configuration

The process for configuring and managing digital certificates is described in the following topics.

Configure Subject Parameters

Subject parameters identify the switch with parameters such as the name, email, company, department, location, and subject name. Subject parameters are the details needed for the certificate signing request (CSR). The resulting certificate is used as part of TLS mutual authentication. The following table defines all required parameters.

Table 6: Required Subject Parameters

Parameter	Value
Common-name	The name of the subject sending the CSR to the certificate authority (CA). Valid entries range from 0 to 64 characters.
Country	The 2-character code of the country of the subject sending the CSR to the CA.
E-mail	The email address of the subject sending the CSR to the CA. Valid entries range from 0 to 254 characters.
Locality	The locality of the subject sending the CSR to the CA. Valid entries range from 0 to 128 characters.
Organization	The organization of the subject sending the CSR to the CA. Valid entries range from 0 to 64 characters.
Province	The state or province of the subject sending the CSR to the CA. Valid entries range from 0 to 128 characters.

Table 6: Required Subject Parameters (continued)

Parameter	Value
Subject-name	Although the system has a default subject (Global) assigned, for the purposes of Common Criteria you assign a unique value as a subject identifier to which the subject parameters are assigned. For the purposes of the examples in the following procedure, the subject-name is `VSPSubject`. Valid entries range from 1 to 45 characters. The subject-name is also used in the Enable X.509 Authentication.
Unit	The organizational unit of the subject sending the CSR to the CA. Valid entries range from 0 to 64 characters.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Configure the subject parameters.

```
(config)# certificate subject subject-name VSPSubject common-name <name>
(config)# certificate subject subject-name VSPSubject country <2-letter-country-code>
(config)# certificate subject subject-name VSPSubject e-mail <email-addr>
(config)# certificate subject subject-name VSPSubject locality <locality>
(config)# certificate subject subject-name VSPSubject organization <organization>
(config)# certificate subject subject-name VSPSubject province <state-or-province>
(config)# certificate subject subject-name VSPSubject unit <organizational-unit>
```

3. Verify the details for the specified subject-name.

```
(config)# show certificate subject subject-name VSPSubject
************************************************************
Command Execution Time: Mon Oct 10 14:52:05 2022 UTC
************************************************************
Subject Name : VSPSubject
Common Name : vsp.test.com
Email Address : test@test.com
Organizational Unit : testing
Organization : Extreme
Locality : Any Town
Province : Ga
Country : US
SAN : E-MAIL - test@test.com
DNS - vs
DNS - vsp.test.com
IP - 10.10.10.10
```

For information about configuring details for the SAN field of the certificate, see Configure Subject Alternative Names.

Configure Subject Alternative Names

You use subject alternative names (SANs) to associate such values as email address, IP address, or FQDN with a certificate. To associate SANs with a certificate, use the subject-name parameter that is associated with a particular certificate and CSR. For more information, see Configure Subject Parameters. For the purposes of the examples

in the following procedure, the subject-name is VSPSubject. The following table defines the SAN parameters. All parameters are optional.

Parameter	Value
DNS	The fully qualified domain name of the switch.
e-mail	The email address of the administrator of the switch.
IP	The IPv4 address of the switch.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Configure the SANs for the switch.

```
(config)(config)# certificate subject-alternative-name dns <dns name>
(config)# certificate subject-alternative-name e-mail <e-mail address>
(config)#certificate subject-alternative-name ip <ip address>

(config)# certificate generate-keypair type rsa size 2048
(config)# certificate generate-keypair key-name VSPKey
```

3. View the configured SANs.

```
(config)# show certificate subject-alternative-name
************************************************************
Command Execution Time: Mon Oct 10 14:49:44 2022 UTC
************************************************************
================================================================
SAN Table
================================================================
TYPE NAME SUBJECT
----------------------------------------------------------------
E-MAIL test@test.com VSP5520-Sub
DNS vs VSP5520-Sub
DNS vsp.test.com VSP5520-Sub
IP 10.10.10.10 VSP5520-Sub
```

SANs that are associated with a specified subject-name are displayed when you run the `show certificate subject subject-name <subject-name>` command, as shown in Configure Subject Parameters.

Generate the Key Pair

You can generate the private and public key pair for RSA cryptography. By default, Fabric Engine generates a 2,048 RSA key when the system starts. You can use this procedure to generate a new RSA key. You can assign a key-name label that makes it easier to determine which key to use. For the purposes of the examples in the following procedure, the key-name is `VSPKey`.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Generate the key pair.

```
(config)# certificate generate-keypair type rsa size 2048
```

3. Display the key.

```
(config)# show certificate key-name VSPkey
*********************************************************
Command Execution Time: Mon Oct 10 14:44:33 2022 UTC
*********************************************************
Key Name: VSPKey
Public Key Value: 00000000000000010000000102000000000301000100000100c953119e
1ea296223b35d39681769a7cc056cc0a78ad481f3b274be2b62114a090ceaee9de72306dfac
84ce11f3a3592f3802e9e803f5a99d62786b59dc03a44bb5580766a6527ca1d85669f6d02645
13ae7155bc6923424c4cd68d15ff20cbf6bca0d1960f0d45cd5db1139e86147f33147c24daf1a
0118054290f9d3411783238183ed8b3edc68e4dd071628a80e0fa64b9b02334506e56a4f36dcc
0e47b3869218d53be3d60663430b86958f33c4fcbe6d66549be66a92877b909fc40d084794f6d
9339afe7b2139ad327f1394a3d0153d1a07657cea7e7c667357275ef888ca6372bd45ceffc096
fcf3dd2eb76f3908584d88d7e143f7a20f92c12f69271
```

Install a Trusted Root Certificate

A certificate authority (CA) issues a root certificate to verify the authenticity of other certificates that a root certificate signs. The root certificate is the first certificate in a chain of trust. You install a root certificate on the switch. Fabric Engine accepts certificates in DER (binary) format only.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Use SCP to move the certificate file from the CA system to the `/intflash/shared/certs` folder on the switch.
3. Install the root certificate into the certificate sub-system.

```
(config)# certificate install-file offline-root-ca-filename <cert-filename>
```

The name of the file can contain no more than 80 characters and must be in *.der format.

Install a CA Certificate

A certificate authority (CA) is a trusted entity that signs and issues digital certificates. CA certificates are signed with a private key that the CA owns. The private key corresponds to a public key in the signed CA certificates. You install a CA certificate on the switch. Fabric Engine accepts certificates in DER (binary) format only.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Use SCP to move the certificate file from the CA system to the `/intflash/shared/certs` folder on the switch.
3. Install the CA certificate.

```
(config)# certificate install-file offline-ca-filename <cert-filename>
```

The name of the file can contain no more than 80 characters and must be in *.der format.

Generate the Certificate-Signing Request

You generate a certificate signing request (CSR) as part of the process of getting the SSL/TLS certificate for the Fabric Engine system. The CSR is generated using a previously generated key-name and subject-name (which includes any SAN details you added). For the purposes of the examples in the following procedure, the key-name is VSPKey and the subject-name is VSPSubject. For more information, see Configure Subject Parameters, Generate the Key Pair , and Configure Subject Alternative Names.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Generate the CSR.

```
(config)# certificate generate-csr subject-name VSPSubject key-name VSPKey
```

3. Confirm that the CSR was generated.

```
(config) # ls /intflash/shared/certs
Listing Directory /intflash/shared/certs:
drwxr-xr-x 2 0 0 504 Oct 10 15:58 ./
drwxr-xr-x 4 0 0 7496 Oct 10 12:10 ../
-rw-r--r-- 1 0 0 1124 Oct 10 15:58 cert_sign_reqvsp.test.com.csr
-rw-r--r-- 1 0 0 1421 Jul 18 15:57 interCA.good.cert.der
-rw-r--r-- 1 0 0 1420 Jul 18 15:57 rootCA.good.cert.der
```

The text in bold is an example of a CSR. The name of your CSR will vary.

Sign the Certificate

You can export and import files using an SCP client. SecureFX® from VanDyke Software is one such client that supports multiple methods of file transfer, including SCP. Certificates can be signed in several platforms. OpenSSL is the most common open-source software to use for this purpose.

1. Use SCP to export the CSR from the `/intflash/shared/certs` folder to the certificate-signing application.
2. Take all appropriate steps to have the certificate signed.
3. Use SCP to import the signed certificate to the `/intflash/shared/certs` folder.
4. If necessary, convert the signed certificate to DER (binary) format.

   Fabric Engine supports certificates that are in DER format. You cannot install a signed certificate that is not in DER format. The following is an example of converting a certificate in PEM format to DER format (on a Linux system).

```
$ openssl x509 -outform der -in <input-filename.pem> -out <output-filename.der>
```

Install a Signed Certificate

The signed certificate is used for mutual authentication with TLS and SSH X.509.

- Ensure you have imported the signed certificate to the /initflash/shared/certs folder. For more information, see Sign the Certificate.

- Ensure that the DNS client is configured and reachable if the OCSP responder in the certificate contains a host name instead of an IP address.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Ensure that the certificate is in the correct folder.

```
(config)# ls /intflash/shared/certs
Listing Directory /intflash/shared/certs:
drwxr-xr-x 2 0 0 504 Oct 10 12:06 ./
drwxr-xr-x 4 0 0 7896 Oct 10 11:33 ../
-rw-r--r-- 1 0 0 1134 Oct 10 11:45 cert_sign_reqvsp5520.test.com.csr
-rw-r--r-- 1 0 0 1421 Oct 10 11:38 interCA.good.cert.der
-rw-r--r-- 1 0 0 1420 Oct 10 11:38 rootCA.good.cert.der
-rw-r--r-- 1 0 0 1291 Oct 10 12:06 vsp5520.test.com.cert.der
(config)#
```

   The text is bold is an example of a signed certificate. Your certificate name will vary.

3. Install the certificate.

```
(config)# certificate install-file offline-subject-file <cert-filename>
```

4. Verify that the certificate was installed.

```
(config)# show certificate cert-type offline-subject-cert
********************************************************************************
Command Execution Time: Tue Oct 11 11:19:55 2022 EDT
********************************************************************************
CERT table entry
Certificate Type : Offline Subject Certificate
VersionNumber : X.509 v3
SerialNumber : 100d
IssuerName : CN:interCA.good, EM:, OU:, O:Extreme, L:, P:, C:US
ValidityPeriodNotBefore : 10/10/2022 20:03:06
ValidityPeriodNotAfter : 10/07/2032 20:03:06
CertificateSignatureAlgorithm : sha256withRSAEncryption
CertificateSignature : <Truncated from guidance document>
Subject : CN:vsp5520.test.com, EM:test@test.com,
OU:Engineering,
O:Extreme, L:Any Town, P:Ca, C:US
SubjectPublicKeyAlgorithm : rsaEncryption
SubjectPublicKey : <Truncated from guidance document>
HasBasicConstraint : 1
HasKeyUsage : 1
IsCa : 0
KeyUsage : 15 digitalSignature nonRepudiation
keyEncipherment
dataEncipherment
ExtendedKeyUsage : TLS Web Client Authentication, TLS Web Server
Authentication,
CDPUrl :
OCSPUrl : http://ocsp.test.com:8082
Revocation Status : unknown
Status : offline-certificate
Installed : 1
CertificateFileName : self_cert_vsp5520.test.com.der
```

Display Configured Key Pairs

You can view the names and public keys of all configured key pairs.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Display the names and public keys of all key pairs.

```
(config)# show certificate key-name
Key Name: pki_key
Public Key Value: 00000000000000010000000102000000000301000100000100bdb1cf8382d66a2d
2d0d24b4477908641c16423c089d9131781a3ada005e52074e1ff3561e29598f93c53dcb06e4d23533557
3419bb938b6ccf93d3e6767d0932e129ea2f556276efce2be825df1f9dc661d3cafee7125f4f7126f5ba7e8
d9029623398b7d3fb00063ea0e4bedd56e276c52a6371b289de3ee4198ff2397b512b516604eac4e5f0f4a0
621d7ac42541491d368f21e17a440aa6130a825a2a7ca6ab1d7a7868f93e4d0d83c7e4973cf204b4f5f654
abbaa9aa6199247976488b0957e65b656a6d21a2a4ac4d322a36c786d8a8deec763b6aec0d05b0f6bfe
87602caecb2cc71e2e4f9f4f8c4d4d4e9b25adf9c02eb44b763542f0449a326d0f3b
Key Name: rsa_2048
Public Key Value: 00000000000000010000000102000000000301000100000100c150b1851644aaae
f08060f3b3a7a0618758b84184867ffd80b3e02ec30676171fe36e99f5450656fc6e6db672b6239f760c
97c3e49639cea5d503c0e478bf7a4d213d5698d09d63622ccb279addbaa34135c81d70660489b55b6babca5
9
4f17d8ed250cf917325df0f73a10896157e6e3a24a584bc713b2e6493d059c8efd53bbbf5db0aa95b43c166
8
ba1053d0fe0e5c44dc889bd35bf11730e5827cb2068048ab97e9f0757514f47332337376eed83a7cb95a534
62639f5a47f026b0172cfa3ddffee7269e737a32d8f2e5590a9ee07d3f329af4e4f2a73ed9de59991
6bc25e6ac51e482cbbb71f736ec0e396fc314e5eed3c438efff68d1a31bdbed24d55
```

Remove a Key

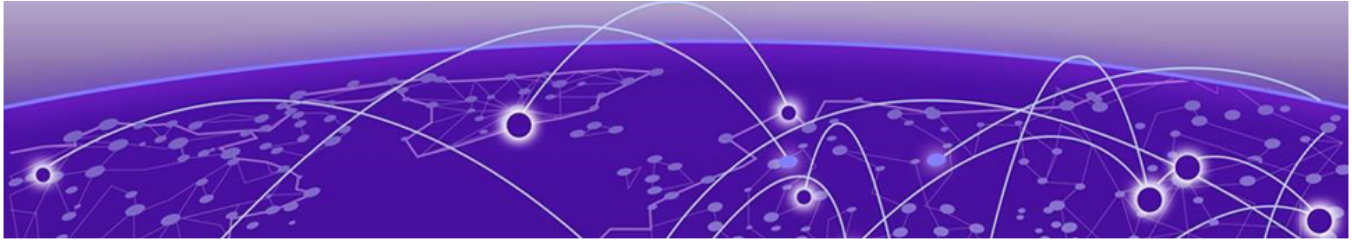
You can remove a key from the certificate store for various reasons, such as a key has been compromised or a policy requires a new key.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Remove the specified key.

```
(config)# no certificate generate-keypair
```



Audit Logs and Syslog

Logging

Transmission of audit logs to the external audit server occurs in real time, with each audit record transferred as it is generated. If the connection to the external audit server is lost, the switch continues to save local audit logs, so there is no loss of audit. An automated log- reconciliation process (syncing) occurs between the locally stored records with the external audit server when the connection is reestablished.

Log-Message Format

Log messages have a standardized format. All system messages are tagged with the following information, except that alarm type and alarm status apply to alarm messages only.

Information type	Description
CPU slot number	Indicates the CP slot where the command is logged.
Time stamp	Records the date and time at which the event occurred. The format is `MM/DD/YY hh:mm:ss.uuu`, where `uuu` is milliseconds. Example: [11/01/10 11:41:21.376].
Host name	The name of the host from which the message is generated.
Event code	Precisely identifies the reported event.

Information type	Description
Alarm code	Specifies the alarm code.
Alarm type	Identifies the type (Dynamic or Persistent) for alarm messages.
Alarm status	Identifies the status (set or clear) for alarm messages.
VRF name	Identifies the Virtual Routing and Forwarding (VRF) instance.
Module name	Identifies the software module or hardware from which the log is generated.
Severity level	Identifies the severity of the message.
Sequence number	Identifies the specific CLI command.
Context	Specifies the type of the session used to connect to the device. For a remote session, the remote IP address is identified.
User name	Specifies the user name that was used to log in to the device.
CLI command	Specifies the commands typed during the CLI session. The system logs anything typed during the CLI session as soon as the user presses the `Enter` key.

The encrypted information in a log file is for debugging purposes. Only a Customer Service engineer can decrypt the encrypted information in a log file. CLI commands display the logs without the encrypted information. Do not edit the log file.

Log Message Severity Levels

The following table describes the system message severity levels.

Severity level and code	Definition
Emergency (0)	A panic condition that occurs when the system becomes unusable. A severity level of Emergency is usually a condition that affects multiple applications or servers. You must correct this condition immediately.
Alert (1)	Any condition requiring immediate attention and correction. You must correct this condition immediately, but this level usually indicates failure of a secondary system, such as an Internet Service Provider connection.
Critical (2)	Any critical condition, such as a hard drive error.

Severity level and code	Definition
Error (3)	A nonfatal condition occurred. You can be required to take appropriate action. For example, the system generates an error message if it is unable to lock onto the semaphore that is required to initialize the IP addresses that are used to transfer the log file to a remote host.
Warning (4)	A nonfatal condition occurred. No immediate action is needed. An indication that an error can occur if action is not taken within a given amount of time.
Notification (5)	Significant event of a normal nature. An indication that unusual, but not error, conditions have occurred. No immediate action is required.
Info (6)	Information only. No action is required.
Debug (7)	Information useful for debugging.
Fatal (0)	A fatal condition occurred. The system cannot recover without restarting. For example, a fatal message is generated after the configuration database is corrupted.

Based on the severity of the message, the platform dispatches each message to one or more of the following destinations:

- Workstation display
- Local log file
- One or more remote hosts

You can log system log messages to external system log hosts with both IPv4 and IPv6 addresses with no difference in functionality or configuration except in the following case. When you configure the system log table in EDM, you must select either IPv4 or IPv6.

Log Files

Log file capture hardware and software log messages and alarm messages. The device logs to internal flash.

The system saves internal log messages in a circular list in memory, which overwrite older log messages as the log fills. Unlike the log messages in a log file, the internal log messages in memory do not contain encrypted information, which can limit the information available during troubleshooting.

Files are stored locally, with maximum capacity based on current available hard-drive space. You should free disk space on the flash if the system generates an alarm based on system thresholds, which are between 75% and 90%:

- 5320 and 5420 devices have a threshold of 90%.

- 7720, 7520, 5720, and 5520 devices have a threshold of 75%.

After disk space usage returns below the device threshold, the system clears the alarm, and then starts logging to a file again.

Log files have the following naming rules:

- The log file name as the following format: `log.xxxxxxxx.sss`. The prefix of the log file name is log. The six characters after the prefix contain the last three bytes of the chassis base MAC address. The next two characters are 01. The last three characters (sss) denote the sequence number of the log file.
- The sequence number of the log file is incremented for each new log file created after the existing log file reaches the maximum configured size.
- At initial system start up when no log file exists, a new log file with the sequence number 000 is created. After a restart, the system finds the newest log file from internal flash based on file timestamps. If the newest log file is on the flash that is used for logging, the system continues to use the newest log file. When the maximum configured size is reached, the system continues to create a new log file with an incremental sequence number on the internal flash for logging.

Enable a TLS Connection to the Syslog Server

Fabric Engine communicates with an external syslog (audit) server by establishing a trusted channel between itself and the audit server. Implementation of the trusted channel employs port forwarding using the Transport Layer Security (TLS) with X.509v3 certificate-based authentication between a remote syslog server and the device. For more information, see X.509 Certificate-Based Authentication.

Take the following steps to set up a remote port forwarding connection between the Fabric Engine device (the client) and the syslog server that is installed on a host that serves as a TLS server.

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Create the syslog host and specify its IPv4 or IPv6 address.

```
(config)# syslog host <host-ID> address <ip-addr>
```

3. Enable the syslog host.

```
(config)# syslog host <host-ID> enable
```

4. Set up secure forwarding in TLS mode.

```
(config)# syslog host <host-ID> secure-forwarding mode tls
server-certname <cert-name>
```

5. Define the TCP port for secure forwarding.

```
(config)# syslog host <host-ID> secure-forwarding tcp-port <port-num>
```

Enable CLI Logging to Syslog

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

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Enable logging.

```
(config)# clilog enable
```

3. Verify the configuration.

```
(config)# show clilog
```

View Log Files

You can view log files by parameters such as file name, category, and severity.

1. Access privileged EXEC mode.

```
# enable
```

2. View a list of log files in order from the oldest to the most recent.

```
# show logging file detail
CP1 [02/06/21 22:38:20.678:UTC] 0x00270428 00000000 GlobalRouter SW INFO Lifecy
cle: Start
CP1 [02/06/21 22:38:21.771:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s oom95 started, pid:4795
CP1 [02/06/21 22:38:22.780:UTC] 0x0027042b 00000000 GlobalRouter SW INFO Proces
s hckServer started, pid:4849
```

This example shows only a few of the many possible log files.

3. View alarm log entries.

```
# show logging file alarm
```

4. View a list of logs organized by the CPU that generated them.

```
# show log file CPU <CPUs>
```

Valid <CPU> values range from 0 to 100 characters. Separate multiple CPUs with a vertical bar. For example: `CPU1|CPU2`.

5. View CLI and SNMP log entries.

```
# show logging file detail
```

6. View logs for a specific event code.

```
# show logging file event-code <code>
```

Valid <code> values range from 0 to 10 characters. Separate multiple codes with a verticle bar.

7. View logs for a specific module.

```
# show logging file module <module>
```

Valid <module> values range from 0 to 100 characters and include the following module categories: SNMP, EAP, RADIUS, RMON, WEB, STG, IGMP, HW, MLT, FILTER, QOS, CLILOG, SW, CPU, IP, VLAN, IPMC, IP-RIP, OSPF, PIM, POLICY, RIP, and SNMPLOG. Separate multiple modules with a vertical bar.

8. View logs for one or more severity levels.

```
# show logging file severity <level>
```

   Valid <level> values range from 0 to 25 characters and include the following: INFO, ERROR, WARNING, FATAL. Separate multiple severity levels with a vertical bar.

9. View a list of log files in order from most recent to oldest.

```
# show logging tail
```

Clear the Log File

You can clear log messages from the log file.

1. Access privileged EXEC mode.

```
# enable
```

2. Clear the file.

```
# clear logging
```

Self-Test Audit Log Records

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

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

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

```
CP1 [02/06/21 22:38:24.717:UTC] 0x000006cc 00000000 GlobalRouter SW INFO
rcStart: FIPS Power Up Self Test SUCCESSFUL - 0
```

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

```
CP1 [02/05/21 12:35:32.911:UTC] 0x000006c3 00000000 GlobalRouter SW INFO rcStart: Failed
to enable FIPS
```

The following is an example of a log entry for a verification audit.

```
1 2022-01-04T18:00:07.393Z VSP-4900-12MXU-12XE IO1 - 0x00264541 - 00000000 GlobalRouter
SW INFO Image Integrity verification passed.
```

Audit Record Samples

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

The following table pairs the text of the audit records from the Fabric Engine switch with the corresponding requirement identifier and event. The record text is the same

for all claimed switches in the evaluated configuration. For a list of the claimed switches, see Evaluated Devices on page 11.

Table 7: Audit record samples

Requirement Identifier	Auditable Event	Audit Record Text
FAU_GEN.1	Start of audit functions	2024-05-27T19:26:54.223Z 5420F-48P-4XE-FabricEngine CP1 - 0x0000065e - 00000003.1 DYNAMIC CLEAR GlobalRouter SW INFO Slot 1: Intflash disk space utilization - below 75%, allow logging to file.
FAU_STG_EXT.1	Configuration of local audit settings	2025-06-05T00:30:15.896Z VOSS5320 CP1 00000000 GlobalRouter CLILOG INFO 141 SSH:172.16.16.252 gssadmin syslog host 1 enable
FAU_GEN.1	Stop of audit functions, 5420 and 5420 (see Log Files on page 42 for device-specific threshold information)	2025-06-24T13:52:36.092Z VOSS5320 CP1 - 0x0000065d - 00000003.1 DYNAMIC SET GlobalRouter SW WARNING Slot 1: Intflash disk space utilization - above 90%, stop logging to file.
FAU_GEN.1	Stop of audit functions, 5520, 5720, 7520, and 7720 (see Log Files on page 42 for device-specific threshold information)	2025-03-03T16:36:18.947Z VOSS5520 CP1 - 0x0000065d - 00000003.1 DYNAMIC SET GlobalRouter SW WARNING Slot 1: Intflash disk space utilization - above 75%, stop logging to file.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FAU_GEN.1	Reset passwords	2024-05-27T18:05:37.958Z 5420F-48P-4XE-FabricEngine CP1 - 0x0000461d - 00000000 GlobalRouter SNMP INFO Admin Password Change success
FCS_NTP_EXT.1	Add time server	2024-02-01T20:47:36.251Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 904 SSH:192.168.144.253 gssadmin ntp server 192.168.144.253 authenable
FCS_NTP_EXT.1	Remove time server	2024-09-26T15:50:44.179Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 10 SSH:192.168.144.253 gssadmin no ntp server 192.168.144.2 authenable
FCS_SSHS_EXT.1	No matching method	SyslogReceipt:2024-11-19T20:56:28.580077-05:00 Host:vsp4900 AuditTimestamp:2025-07-11T14:01:08.351Z VOSS5320 CP1 - 0x000d8602 - 00000000 GlobalRouter SSH INFO SSH Max Packet Size 35840 Exceeded user GssTestUser on host 172.16.16.254, session_id = 0.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FCS_SSHS_EXT.1	Oversized packet	2024-07-18T18:33:18.147Z 5420F-48P-4XE-FabricEngine CP1 - 0x000d8602 - 00000000 GlobalRouter SSH INFO SSH Max Packet Size 32768 Exceeded user gssadmin on host 192.168.144.253.
FCS_SSHS_EXT.1	Rekey for time	2024-07-12T22:38:14.901Z 5420F-48P-4XE-FabricEngine CP1 - 0x000d8633 - 00000000 GlobalRouter SSH INFO SSH Server: Rekey initiated because time exceeds 3600 seconds.
FCS_SSHS_EXT.1	Rekey for volume	2024-07-12T18:57:26.575Z vsp8400 CP1 - 0x000d8632 - 00000000 GlobalRouter SSH INFO SSH Server: Rekey initiated because transmitted data exceeds 1000000000 bytes.
FCS_TLSC_EXT.1	Wrong extended key usage value	2024-07-15T18:06:55.774Z 5420F-48P-4XE-FabricEngine CP1 - 0x00070635 - 00000000 GlobalRouter SW ERROR SYSLOG Extended key usage mismatch. The extended key usage extension does not have the TLS Web Server Authentication purpose set.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FCS_TLSC_EXT.1	Signature algorithm mismatch	2025-06-10T22:08:15.732Z VOSS5320 CP1 00000000 GlobalRouter SW ERROR TLS handshake between Syslog Client and Server failed with status=ERR_CERT_INVALID_SIGNATURE
FCS_TLSC_EXT.1	No matching cipher	2025-06-05T22:03:27.462Z VOSS5320 CP1 00000000 GlobalRouter SW ERROR TLS handshake between Syslog Client and Server failed with status=ERR_SSL_NO_CIPHER_MATCH
FCS_TLSC_EXT.1	Wrong TLS version	2024-07-15T17:52:30.528Z 5420F-48P-4XE-FabricEngine CP1 - 0x00070618 - 00000000 GlobalRouter SW ERROR TLS handshake between Syslog Client and Server failed with status=ERR_SSL_PROTOCOL_V ERSION.
FCS_TLSC_EXT.1	Handshake error	2024-12-20T13:47:10.837Z 5420F-48P-4XE-FabricEngine CP1 CP100000000 GlobalRouter SW ERROR TLS handshake between Syslog Client and Server failed with status= ERR_SSL_FATAL_ALERT_HAND SHAKE_FAILURE.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FCS_TLSC_EXT.1	Bad record MAC	2024-02-16T22:10:59.918Z 5420F-48P-4XE-FabricEngine CP1 - 0x00070629 - 00000000 GlobalRouter SW ERROR Fatal alert - SSL_ALERT_BAD_RECORD_MA C detected during TLS negotiation with IP 192.168.144.253.
FIA_AFL.1	Failed login due to exceeding limit	2025-06-05T22:01:51.142Z VOSS5320 CP1 - 0x000d8616 - 00000000 GlobalRouter SSH ERROR connection denied: overall max SSH sessions reached or number of logins exceeded for user:gssadmin.
FIA_UAU_EXT.2	All use of identification and authentication mechanisms	See FIA_UIA_EXT.1.
FIA_UIA_EXT.1	Successful console login	2024-08-10T13:52:13.135Z 5420F-48P-4XE-FabricEngine CP1 - 0x000305ca - 00000000 GlobalRouter SW INFO user gssadmin connected by console port.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FIA_UIA_EXT.1	Failed console login	022-08-10T13:49:27.518Z 5420F-48P-4XE-FabricEngine CP1 - 0x001985a6 - 00000000 GlobalRouter ACLI WARNING Unauthorized login attempt with the user gssadmin and the number of unsuccessful attempts are: 1 and unsuccessful login attempt time is: Wed Aug 10 13:49:27 2024
FIA_UIA_EXT.1	Failed console login	2024-08-10T13:49:27.518Z 5420F-48P-4XE-FabricEngine CP1 - 0x001985a0 - 00000000 GlobalRouter ACLI WARNING Blocked unauthorized ACLI access for user gssadmin from console port.
FIA_UIA_EXT.1	Successful SSH/CLI login (Password)	SyslogReceipt:2024-11-19T20:49:37.368157-05:00 Host:vsp4900 AuditTimestamp:2024-11-20T01:49:36.016Z SyslogMessage:CP10 0000000 GlobalRouter SSH INFO SSH user authentication succeeded for user gssadmin on host 192.168.144.254.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FIA_UIA_EXT.1	Failed SSH/CLI login (Password)	SyslogReceipt:2024-11-19T20:49:51.688973-05:00 Host:vsp4900 AuditTimestamp:2024-11-20T01:49:50.336Z SyslogMessage:CP10 0000000 GlobalRouter SSH WARNING Unauthorized login attempt with the user gssadmin and the number of unsuccessful attempts are: 1 and unsuccessful login attempt time is: Sat Nov 20 01:49:50 2024.
FIA_UIA_EXT.1	Failed SSH/CLI login (Password)	SyslogReceipt:2024-11-19T20:49:51.689463-05:00 Host:vsp4900 AuditTimestamp:2024-11-20T01:49:50.336Z SyslogMessage:CP10 0000000 GlobalRouter SSH INFO SSH invalid username/password for user gssadmin on host 192.168.144.254.
FIA_UIA_EXT.1	Successful SSH/CLI login (Public Key)	2024-07-11T20:18:41.605Z 5420F-48P-4XE-FabricEngine CP1 - 0x000d8602 - 00000000 GlobalRouter SSH INFO SSH RSA Public Key authentication succeeded for user operator on host 192.1 68.144.253.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FIA_UIA_EXT.1	Failed SSH/CLI login (Public Key)	SyslogReceipt:2024-11-19T20:54:36.005444-05:00 Host:vsp4900 AuditTimestamp:2024-11-20T01:54:34.651Z SyslogMessage:CP10 0000000 GlobalRouter SSH INFO SSH RSA Public Key authentication failed for user gssadmin on host 192.168.144.254.
FIA_UIA_EXT.1	Successful SSH/CLI login (X509 Certificate)	2024-08-23T14:21:56.327Z 5420F-48P-4XE-FabricEngine CP1 - 0x000d8602 - 00000000 GlobalRouter SSH INFO SSH X509 certificate authentication succeeded for user GssTestUser on host 192.168.144.253
FIA_UIA_EXT.1	Failed SSH/CLI login (X509 Certificate)	2024-09-14T15:14:47.353Z 5420F-48P-4XE-FabricEngine CP1 - 0x000d8602 - 00000000 GlobalRouter SSH INFO SSH X509 certificate authentication failed for user GssTestUser on host 192.168.144.253.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FIA_X509_EXT.1/Rev	Add trust anchor	2024-12-20T16:24:44.058Z 5420F-48P-4XE-FabricEngine CP1 CP100000000 GlobalRouter SW INFO SYSLOG: Successfully added the certificate rootca-rsa to the Syslog Trusted Anchor.
FIA_X509_EXT.1/Rev	Remove trust anchor	2024-12-14T12:06:09.515824-05:0 0 Host:vsp4900 AuditTimestamp:2024-12-14T17:06:25.845Z SyslogMessage:CP100000000 GlobalRouter SW INFO SYSLOG: Successfully removed the certificate rootca-rsa from the Syslog Trusted Anchor.
FIA_X509_EXT.1/Rev	CN does not match	2024-07-20T18:18:30.538Z 5420F-48P-4XE-FabricEngine CP1 - 0x00070632 - 00000000 GlobalRouter SW ERROR SYSLOG Common name mismatch. Peer certificate common name: tl27-16b.example.com - Configured server-cert-name: tl27-16b.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FIA_X509_EXT.1/Rev	Invalid EKU	2024-02-16T19:30:59.504Z 5420F-48P-4XE-FabricEngine CP1 - 0x00070635 - 00000000 GlobalRouter SW ERROR SYSLOG Extended key usage mismatch. The extended key usage extension doesn't have the TLS Web Server Authentication purpose set.
FIA_X509_EXT.1/Rev	Basic constraints missing for CA (SSH)	2024-10-27T13:31:20.595Z 5420F-48P-4XE-FabricEngine CP1 - 0x003a8675 - 00000000 GlobalRouter DIGITALCERT ERROR Invalid Certificate! Details = [Invalid Basic Constraints] 2024-10-27T13:31:20.595Z 5420F-48P-4XE-FabricEngine CP1 - 0x000d8602 - 00000000 GlobalRouter SSH INFO SSH authentication ended unexpectedly for user GssTestUser on host 192.168.144.253
FIA_X509_EXT.1/Rev	Basic constraints false for CA (SSH)	Same as "basic constraints missing for CA (SSH)".

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FIA_X509_EXT.1/Rev	Basic constraints missing for CA (Syslog)	2024-07-22T16:48:30.536Z 5420F-48P-4XE-FabricEngine CP1 - 0x00070618 - 00000000 GlobalRouter SW ERROR TLS handshake between Syslog Client and Server failed with status=ERR_CERT_INVALID_CERT_POLICY.
FIA_X509_EXT.1/Rev	Basic constraints false for CA (Syslog)	Same as "basic constraints missing for CA (Syslog)".
FIA_X509_EXT.1/Rev	Certificate revoked	1 2024-07-20T15:38:30.654Z 5420F-48P-4XE-FabricEngine CP1 - 0x00070629 - 00000000 GlobalRouter SW ERROR Fatal alert - SSL_ALERT_CERTIFICATE_REVOKED detected during TLS negotiation with IP 192.168.144.253.
FIA_X509_EXT.1/Rev	Expired certificate	2024-12-20T14:51:37.937Z 5420F-48P-4XE-FabricEngine CP1 CP100000000 GlobalRouter SW ERROR Fatal alert - SSL_ALERT_CERTIFICATE_EXPIRED detected during TLS negotiation with IP 192.168.144.253.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FMT_MOF.1/Manual Update	Manual update attempts (trusted update)	2024-02-03T21:17:26.936Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 202 CONSOLE gssadmin software add VOSS4900.8.3.100.0int083.tgz 2024-02-16T04:26:02.768Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 4 CONSOLE gssadmin software activate VOSS4900.8.3.100.0int089
FMT_SMF.1	Local and remote system administration	See FIA_UIA_EXT.1
FPT_STM_EXT.1	Discontinuous time changes	2024-12-21T14:28:26.006Z 5420F-48P-4XE-FabricEngine CP1 - 0x0003064a - 00000000 GlobalRouter SW INFO Clock set successfully. New time:Tue Dec 21 14:28:26 2024 UTC, Prev time: Sat Nov 11 11:11:14 2000 UTC,Initiated by SSH, user: gssadmin from IP: 192.168.144.253.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text	
FPT_TUD_EXT.1	Software signature verification failed	2024-08-25T14:42:07.818Z 5420F-48P-4XE-FabricEngine CP1 - 0x00264511 - 00000000 GlobalRouter SW INFO Image signature verification FAILED user gssadmin.	
FPT_TUD_EXT.1	FPT_TUD_EXT.1	Software signature verification passed	2025-06-27T17:36:07.000Z VOSS5320 CP1 - 0x00264511 - 00000000 GlobalRouter SW INFO Image signature verification PASSED user gssadmin
FTA_SSL.3	Remote session termination	2024-01-03T20:40:15.282Z 5420F-48P-4XE-FabricEngine CP1 - 0x0003067a - 00000000 GlobalRouter SW INFO User gssadmin forced logout after CLI session inactivity of 180 seconds.	
FTA_SSL.4	SSH logout	2024-09-15T16:13:22.718Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 433 SSH: 192.168.144.253 gssadmin logout.	
FTA_SSL.4	Console logout	2024-01-03T20:40:24.090Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 486 CONSOLE gssadmin logout.	

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FTA_SSL_EXT.1	Forced lockout after CLI inactivity	2024-09-23T14:08:13.454Z vsp7400 CP1 00000000 GlobalRouter SW INFO User gssadmin forced log-out after CLI session inactivity of 63 seconds.
FTP_ITC.1	TLS client session establishment	2024-12-20T13:49:48.587Z 5420F-48P-4XE-FabricEngine CP1 - 0x00070619 - 00000000 GlobalRouter SW INFO TLS handshake successful between Syslog Client and Server 192.168.144.253.
FTP_ITC.1	TLS client session termination	2024-12-20T13:47:57.318Z 5420F-48P-4XE-FabricEngine CP1 CP100000000 GlobalRouter SW INFO TLS Connection closed between Syslog Client and Server 192.168.144.253.
FTP_ITC.1	TLS client session failure	See FCS_TLSC_EXT.1.
FTP_TRP.1/Admin	SSH session establishment	SyslogReceipt:2024-11-19T20:49:37.868114-05:00 Host:vsp4900 AuditTimestamp: 2024-11-20T01:49:36.018Z SyslogMessage: CP100000000 GlobalRouter SSH INFO SSH CLI session start: user gssadmin on host 192.168.144.254.

Table 7: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FTP_TRP.1/Admin	SSH session termination	SyslogReceipt:2024-11-19T20:49:38.875939-05:00 Host:vsp4900 AuditTimestamp: 2024-11-20T01:49:37.371Z SyslogMessage: CP100000000 GlobalRouter SSH INFO SSH session closed by user gssadmin on host 192.168.144.254.
FTP_TRP.1/Admin	SSH session failure	See FCS_SSHS_EXT.1.

Audit Records for Administrative Actions

Administrative actions generate the following audit records on the Fabric Engine switch.

The record text is the same for all claimed switches in the evaluated configuration. For a list of the claimed switches, see Evaluated Devices.

Table 8: Administrative action records

Admin Action	Scenario or Command	Audit Record Text
Log-in	Connected through console port	2024-12-20T13:39:40.588Z 5420F-48P-4XE-FabricEngine CP1 CP100000000 GlobalRouter SW INFO user gssadmin connected through console port
Log in	Logged in	2025-01-07T13:34:21.144206-05:00 Host:vsp4900 AuditTimestamp :2025-01-07T18:34:20.277Z SyslogMessage:CP100000000 GlobalRouter SW INFO user gssadmin logged in through ssh,Unsuccessful Login attempts from last login i s:0 and Last Successful Login time is:Fri Jan 7 18:33:47 2025

Table 8: Administrative action records (continued)

Admin Action	Scenario or Command	Audit Record Text
Log out	Logged out from console port	2024-12-21T20:15:20.840Z 5420F-48P-4XE-FabricEngine CP1 - 0x00030637 - 00000000 GlobalRouter SW INFO user gssadmin logged out from console port
Log out	SSH CLI session end	2025-01-07T13:34:28.970645 -05:00 Host:vsp4900 AuditTimestamp :2025-01-07T18:34:27.744Z SyslogMessage:CP100000000 GlobalRouter SSH INFO SSH CLI session end: user gssadmin on host 192.168.144.253
Configure SSH rekey (volume)	ssh rekey datalimit	2025-07-11T18:59:33.168Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 1380 CONSOLE gssadmin ssh rekey data-limit 1
Configure SSH rekey (time)	ssh rekey timeinterval	2025-07-11T18:59:04.183Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 1377 CONSOLE gssadmin ssh rekey time-interval 1
NTP server config	Enable NTP server	2025-06-13T14:37:05.606Z VOSS5320 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 318 SSH:172.16.16.254 gssadmin ntp
NTP server config	Disable NTP server	2025-06-15T08:46:26.346Z VOSS5320 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 418 SSH:172.16.16.254 gssadmin no ntp

Table 8: Administrative action records (continued)

Admin Action	Scenario or Command	Audit Record Text
Manually specify clock value	set clock	2024-12-21T14:28:26.006Z 5420F-48P-4XE-FabricEngine CP1 - 0x0003064a - 00000000 GlobalRouter SW INFO Clock set successfully. New time:Tue Dec 21 14:28:26 2024 UTC, Prev time:Sat Nov 11 11:11:14 2000 UTC,Initiated by SSH, user: gssadmin from ip: 192.168.144.253
Trusted update	software add	2025-02-03T21:17:26.936Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 202 CONSOLE gssadmin software add VOSS4900.8.3.100.0int083.tgz
Trusted update	software activate	2025-02-16T04:26:02.768Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 4 CONSOLE gssadmin software activate VOSS4900.8.3.10 0.0int089
Set timeout value	Set CLI timeout	2025-09-15T16:13:19.705Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 428 SSH:192.168.144.253 gssadmin cli timeout 7200
Ability to configure the access banner	banner custom	2025-05-28T20:18:48.328Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 35 SSH:192.168.144.253 gssadmin banner custom
Ability to configure the session inactivity time before session termination or locking	ssh timeout	2024-12-23T14:34:13.128Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 117 SSH:192.168.144.253 gssadmin ssh timeout 60

Table 8: Administrative action records (continued)

Admin Action	Scenario or Command	Audit Record Text
Ability to update the system, and to verify the updates using [digital signature] capability before installing those updates	Image signature verification PASSED	2025-06-27T17:36:07.000Z VOSS5320 CP1 - 0x00264511 - 00000000 GlobalRouter SW INFO Image signature verification PASSED user gssadmin
Ability to update the system, and to verify the updates using [digital signature] capability before installing those updates	Image signature verification FAILED	2025-08-16T17:25:27.898Z 5420F-48P-4XE-FabricEngine CP1 - 0x00264511 - 00000000 GlobalRouter SW INFO Image signature verification FAILED
Ability to configure the authentication failure parameters for FIA_AFL.1	default-lockout-retries	2024-12-21T19:19:58.467Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 64 CONSOLE gssadmin password default-lockout-retries 3
Ability to modify the behavior of the transmission of audit data to an external IT entity	Enable syslog	2025-01-07T13:41:33.436018-05:00 Host:vsp4900 AuditTimestamp :2025-01-07T18:41:32.567Z SyslogMessage:CP100000000 GlobalRouter CLILOG INFO 1033 SSH:192.168.144.253 gssadmin syslog host 1 enable
Ability to manage the cryptographic keys	generate-keypair	2025-08-16T18:38:12.779Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 Glob CLILOG INFO 16589 CONSOLE gssadmin certificate generate-keypair type rsa size 2048 key?
Ability to configure the cryptographic functionality	ssh x509v3- auth enable	2025-02-09T21:07:13.864Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 105 SSH:192.168.144.253 gssadmin ssh x509v3-auth enable

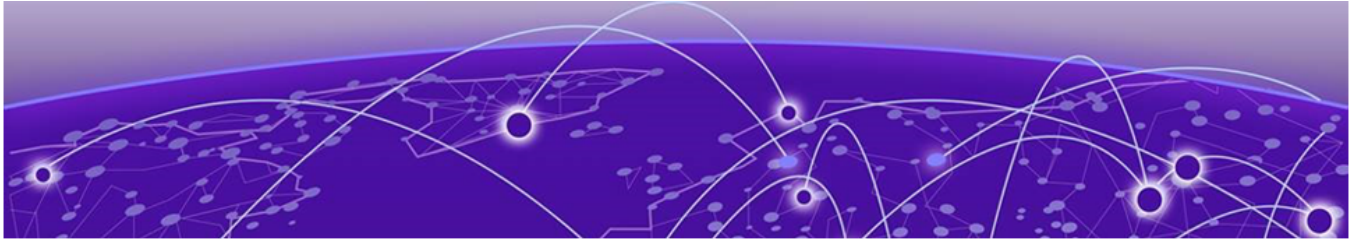
Table 8: Administrative action records (continued)

Admin Action	Scenario or Command	Audit Record Text
Ability to manage the system's trust store and designate X509.v3 certificates as trust anchors,	ssh x509v3- auth ca-name	2025-07-12T18:53:35.209Z VOSS5320 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 75 CONSOLE gssadmin ssh x509v3-auth cert-subject-name VOSS5320
Ability to import X509 v3 certificates to the system's trust store	certificate install-file offline-ca-filename	2025-09-23T17:48:47.608Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 775 SSH:192.168.144.253 gssadmin certificate install-file offlineca-filename subca-rsa.der
Ability to manage the trusted public keys database	ssh install-user-key	2025-11-18T01:37:36.119Z 5420F-48P-4XE-FabricEngine CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 1939 CONSOLE gssadmin ssh install-user-key operator public rsa
Ability to configure NTP	ntp enable	2024-12-22T17:24:01.811Z 5420F-48P-4XE-FabricEngine CP1 - 0x000c8587 - 00000000 GlobalRouter SW INFO NTP Enabled
Ability to re-enable an administrator account		2025-06-20T09:53:40.626Z VOSS5320 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 575 CONSOLE gssadmin password enable-user user-name gssadmin
Ability to configure local audit behavior		2025-06-25T12:50:12.102Z VOSS5320 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 80 SSH:172.16.16.254 gssadmin logging level 0
Ability to set the time which is used for time stamps		2025-06-15T08:45:38.287Z VOSS5320 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 407 SSH:172.16.16.254 gssadmin clock set 06162025142540

Table 8: Administrative action records (continued)

Admin Action	Scenario or Command	Audit Record Text
Ability to configure the reference identifier for the peer		2025-07-02T15:35:09.224Z VOSS5320 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 27 CONSOLE gssadmin certificate subject-alternative-name subject-name GSS dns VOSS53 20.example.com
Ability to generate certificate sign request (CSR) and process CA certificate response		2025-07-16T12:28:24.908Z VOSS5320 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 13 SSH:172.16.16.254 gssadmin certificate generate-csr
Ability to administer the TOE locally	2025-07-08T17:42:50.980Z VOSS5320 CP1 - 0x002c0600 - 00000000 Global Router CLILOG INFO 54 CONSOLE gssadmin cli timeout 7200	

The record text is the same for all claimed switches in the evaluated configuration. For a list of the claimed switches, see Common Criteria Certification Configuration on page 10.



General Configuration Tasks

Overview

This section describes processes for disabling services, creating banner messages, setting an inactivity threshold, and upgrading software.

Disable Unsupported Services

To meet Common Criteria requirements, disable the following services: HTTP, HTTPS, and iqagent.

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Disable HTTP web access

```
(config)# no web-server enable
```

3. Disable HTTPS web access.

```
(config)# no web-server secure-only
```

4. Disable the iqagent application.

```
(config)# application
(config-app)# no iqagent enable
```

Configure the Banner Message

Banner messages provide information to users who access the Fabric Engine command-line interface. Take the following steps to configure the message that users see before they log in and the message of the day that they see after they log in.

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Enable the device to use a custom banner.

```
(config)# banner custom
```

3. Create the custom banner, which users see before they log in.

```
(config)# banner <message-text>
```

Tip
To create a message with multiple lines, use the **banner** command before each new line of the message. To create a string of words separated by spaces, surround the text in quotation marks.

4. Create a message of the day, which users see after they log in.

```
(config)# banner motd <message-text>
```

5. Enable the message of the day.

```
(config)# banner displaymotd
```

6. Save your messages.

```
(config)# save config
```

7. To verify your messages, run the **show banner** command.

The following example creates a custom banner message, "Company, www.Companyname.com," and a message of the day: "Unauthorized access to this system is forbidden. Please log out now."

```
device# enable
device# configure terminal
device (config)# banner custom
device (config)# banner Company
device (config)# banner www.Companyname.com
device (config)# banner motd "Unauthorized access to this system is forbidden."
device (config)# banner motd "Please log out now."
device (config)# banner displaymotd
device (config)# save config
```

Configure a Session Inactivity Timeout Threshold

You can specify the maximum number of seconds allowed for an SSH session or serial connection to be inactive. If inactivity exceeds that threshold, the session is disconnected and the user must log in again.

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Specify the timeout threshold.

```
(config)# cli timeout <seconds>
```

Valid values range from 30 to 655535. The default is 900.

Software Upgrade

- Obtain the upgrade files from the Extreme Networks support site: http://www.extremenetworks.com/support. Access requires a valid user or site ID and a password.
- Back up your configuration files.
- Determine whether you will use an FTP or SFTP application or a USB device to transfer the upgrade files to the device.
- Move all configurations for VLANs above 4059 to another VLAN. Only VLANs in the range of 2 through 4059 are supported. Configurations for VLANs above 4059 are lost after upgrade.

Software upgrade configurations are case sensitive.

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. To use FTP or SFTP to transfer the upgrade files, take the following preparatory steps.
   a. Start the FTP daemon on the device.
   b. Enable the FTPD flag for FTP, the SSHD flag for SFTP, or the flag for SCP.

```
# boot config flags <ftpd|sshd>
```

3. Download the upgrade files to the device using FTP or SFTP or transfer the files through the USB port.

   For an FTP or SFTP session, use the same user name and password that you use to Telnet or SSH to the device.

   Note
   The use of FTP is not covered in this evaluation.

4. Exit global configuration mode.

```
# exit
```

   The device is now in privileged EXEC mode.

5. Extract the upgrade files.

```
# software add <version> -y
```

   The files are extracted to the `/intflash/release` directory.

6. Upgrade the software.

```
# software activate <version>
```

7. Restart the device.
8. Access privileged EXEC mode.

```
# rwa
# enable
```

9. Verify that the software is upgraded.

```
# show software
```

10. Commit the software, which ensures that the software release is trusted.

```
# software commit
```

Display Software Inventory

As a best practice, verify the version of the running software before you begin the upgrade process.

1. Access privileged EXEC mode.

```
# enable
```

2. Verify the running version of the software.

```
# show software
```

The following is an example of output from the `show software` command. The phrase `Primary Release` identifies the active running software.

```
# show software
*************************************************************
Command Execution Time: Mon Oct 17 13:41:27 2024 EDT
*************************************************************
software releases in /intflash/release/
*************************************************************
5520.9.1.100.0int020 (Signed Release)
5520.9.1.100.0int019 Backup Release (Signed Release)
5520.9.1.100.0int018 (Primary Release) (Signed Release)
-------------------------------------------------------------
Auto Commit : enabled Commit Timeout : 10 minutes
```