Extreme VOSS Common Criteria Configuration Guide

8.3.100

9037337-00 Rev AA
December 2022

Legal Notice

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

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

Trademarks

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

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

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

Open Source Declarations

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

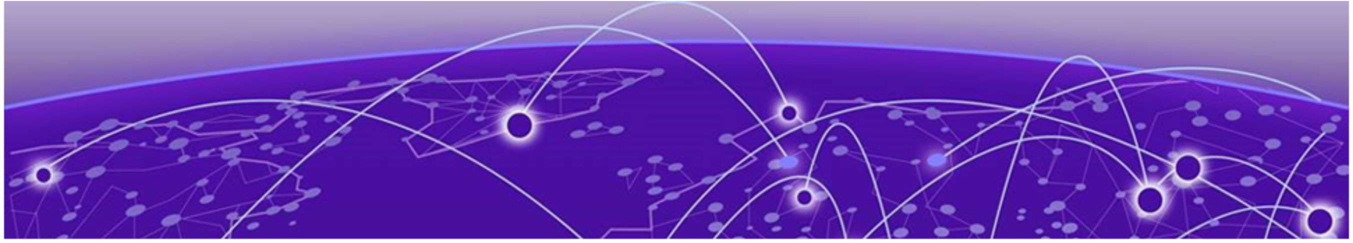
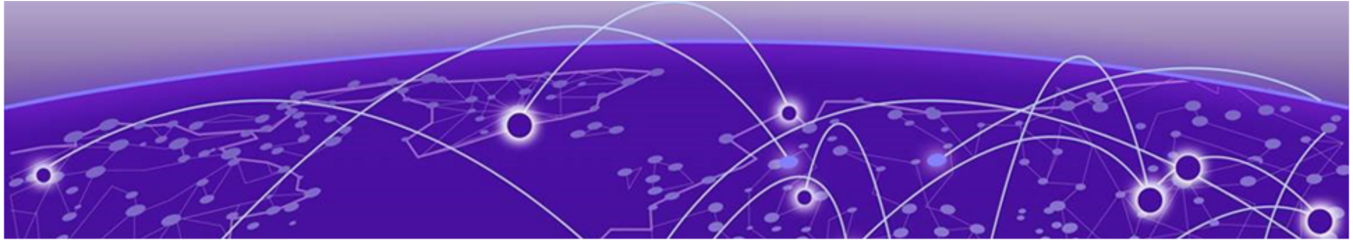


Table of Contents



Preface

Read the following topics to learn about:

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

Text Conventions

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

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

Table 1: Notes and warnings

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

Table 2: Text

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

Table 3: Command syntax

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

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation

Release Notes

Hardware and software compatibility for Extreme Networks products

Extreme Optics Compatibility

Other resources such as white papers, data sheets, and case studies

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

Help and Support

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

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

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

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

Subscribe to Product Announcements

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

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

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

Send Feedback

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

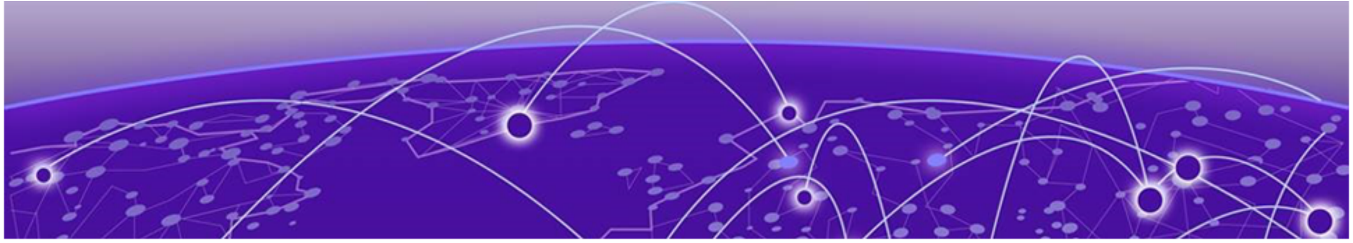
- Content errors, or confusing or conflicting information.

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

To send feedback, do either of the following:

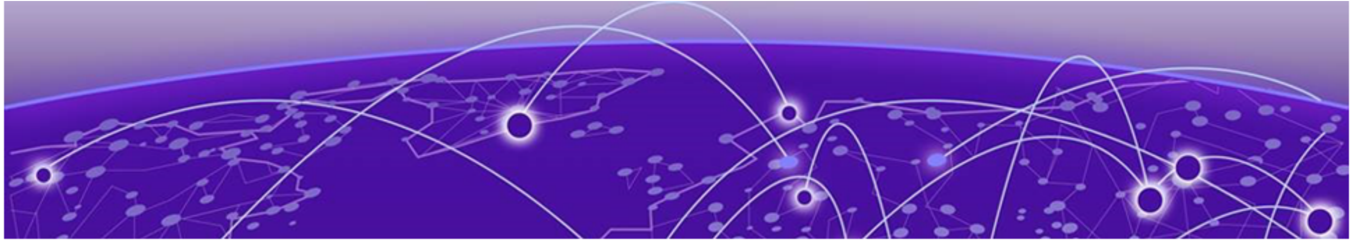
- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

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



About This Document

This document is new for the 8.3.100 release.



Common Criteria Certification Configuration

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

Overview

When administrators log in with role-based credentials, their access is limited to commands they have privileges and permissions to use based on the Common Criteria standards. Network management communication paths are protected against modification and disclosure by SSHv2. For more information, see Secure Shell Configuration on page 23.

In an evaluated configuration, VOSS supports only a trusted channel to an external audit server (a syslog server). That trusted channel must be configured to be protected by TLS. For more information, see Enable a TLS Connection to the Syslog Server on page 42.

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 VOSS version 8.3.100. Cryptographic Algorithm Validation System (CAVS) certifies all cryptographic algorithms required by and used in Common Criteria.

The topics in this guide describe the process of configuring your system to comply with Common Criteria standards.

Evaluated Devices

The following devices, running VOSS 8.3.100, were evaluated for compliance.

Platform	Model
VSP 4900 Series	VSP4900-48P
	VSP4900-24S
	VSP4900-24XE
	VSP4900-12MXU-12XE
VSP 7400 Series	VSP7400-32C
	VSP7400-48Y-8C
VSP 8000 Series	VSP8404C
ExtremeAccess 1400 Series	XA1440
	XA1480

Supported Cryptographic Methods

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

TLS

The switch supports TLS 1.2 as defined in RFC 5246. TLS 1.0 and 1.1 are not supported. For more information, see Enable a TLS Connection to the Syslog Server on page 42.

The following TLS ciphers are supported.

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
- 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

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 on page 23.

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.

- HMAC-SHA1
- HMAC-SHA2-256

The switch performs the SSH key exchange with the Diffie-Hellman-Group14-SHA1 method.

Initial Switch Configuration Tasks

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

1. Establish a serial connection.
2. Log on to the system and change the administrator credentials.
3. Set the management IP address.
4. Configure boot flags.
5. Configure enhanced secure mode, including user accounts and credentials.
6. Set the system date and time.
7. Set up Network Time Protocol.
8. Configure DNS.
9. Configure SSHv2, including host key, encryption types, and authentication methods.
10. Configure and manage certificates.
11. Configure logging.
12. Disable unsupported services.
13. Configure an inactivity timeout.

Access to the Switch

In the evaluated configuration, administrators must use one of the following methods to access and manage the switch.

Serial connection

> You can connect a terminal to the serial console interface. The serial connection is described in Establish a Serial Connection on page 13.
>
> Provide the appropriate administrative credentials to gain access to the switch. You can close a connection by running the **`exit`** or **`logout`** command.

SSHv2

> You can access the switch from a remote client by using the **`ssh`** command in an SSHv2-protected CLI session, which employs certificates, passwords, and public keys for authentication.

You can close a session by running the **`exit`** or **`logout`** command.

For more information, see Secure Shell Configuration on page 23 and Certificate Management on page 30.

Establish a Serial Connection

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

Before You Begin

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

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

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

Procedure

1. Configure the terminal protocol as follows.

   9600 baud for VSP8404C
   115200 baud for VSP 4900 series, VSP 7400 series, and XA 1400 series
   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 switch.
3. Connect the other end of the cable to the terminal or computer serial port.
4. Turn on the terminal.
5. Provide the appropriate administrative credentials to gain access to the switch.

   For related information, see Initial System Log-in and Credential Change on page 13.
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 `admin` and the default password of `admin`.

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 user name and password.
Change the user name and password to continue.
```

```
Enter the new name : rwa
Enter the New password : ****************
Re-enter the New password : ****************

Password changed successfully Last Successful Login:Wed Oct 14 12:20:42 2015
Unsuccessful Login attempts from last login is: 0
```

Set the Management IP Address

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

About This Task

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 *VOSS User Guide* for version 8.2 or later.

> Note
> You can also use an in-band port with a loopback or management VLAN. However, this procedure describes the out-of-band method.

Procedure

1. Access out-of-band configuration mode.

   ```
   # enable
   # configure terminal
   # 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. Enable the out-of-band interface.

   ```
   # enable
   ```

5. Verify the management IP interface information.

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

Configure Boot Flags

The VOSS operating system has several flags that control certain services during system boot.

About This Task

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 the 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 or 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

Procedure

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.

3. Compare the setting of each flag in the table with the list from step 2.
4. To change the setting of a flag to meet the CC requirement, run the command associated with that flag.

Enhanced Secure Mode

Enhanced secure mode enables role-based access control (RBAC) and requires strong password complexity. Enhanced secure mode is required in a Common Criteria configuration.

Role-based Access Control

After you enable enhanced secure mode (see Enable Enhanced Secure Mode on page 17), the switch supports RBAC and five access levels, each with its own set of permissions.

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 role of administrator configures the log in credentials for other users, based on their roles. For more information, see Create User Accounts on page 17 and Configure User Passwords on page 17.

In enhanced secure mode, there can be only one user per role.

Table 5: RBAC levels

Role	Description
Administrator	Has access to all **`configuration`** and **`show`** commands. Can view the log file and security commands. The administrator role is the highest level of user roles. The Privilege and Admin roles do not enforce a lockout on the console, so as to prevent loss of administrative access to the system.
Privilege	Has the same permission set as the administrator, but can only be authenticated locally within the switch. This level is also known as *emergency-admin*. A user with the Privilege role can re-enable a locked-out account. The Privilege and Admin roles do not enforce a lockout on the console, so as to prevent loss of administrative access to the system.
Operator	Has access to all configurations for packet forwarding on Layer 2 and Layer 3. Has access to **`show`** commands to view the configuration. Cannot view audit logs. Cannot access security and password commands.
Auditor	Can view audit logs and all configurations except password configuration.
Security	Has access to security settings and can view the configurations.

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 on page 18 and Enable a Locked-Out User Account on page 19.

Enable Enhanced Secure Mode

In a Common Criteria configuration, you must enable enhanced secure mode in non-JITC sub-mode.

Procedure

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 switch.

```
(config)# exit
# boot
```

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.

About This Task

For more information about user roles, see Enhanced Secure Mode on page 15.

Procedure

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
```

Example

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.

About This Task

For more information about password requirements, see Enhanced Secure Mode on page 15.

Procedure

1. Access 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
   ```

Example

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

```
# enable
# configure terminal
(config)# password set-password user-name bakers
Enter the New password : ********
Password modified for user bakers
(config)# save config
```

Configure Global Password Settings

You can configure the minimum password length and the number of failed password attempts before lockout.

About This Task

These settings affect all users.

Procedure

1. Access global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Set the minimum password length for all users.

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

   Acceptable values range from 8 to 32. The default is 15.

3. Configure the number of retries after a failed log-in attempt that can occur before a user is locked out.

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

   Acceptable values range from 1 to 255.

   Note
   Only the user with the Privilege role can re-enable a locked-out account. For more information, see Enable a Locked-Out User Account on page 19.

4. 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.

Procedure

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Enabled the locked-out account.

```
(config)# password enable-user user-name {admin | operator | security | auditor}
```

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.

About This Task

As a best practice, do not update the time manually when the VOSS switch is acting as a client of an external Network Time Protocol (NTP) server. For more information, see Network Time Protocol on page 19.

Procedure

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

```
# clock set <MMddyyyhhmmss>
```

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

Network Time Protocol (NTP) synchronizes the internal clocks on devices across a network.

Overview

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

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

VOSS version 8.3.100 uses NTPv4.

For complete information about NTP as it relates to VOSS, see the VOSS User Guide.

Limitations and requirements

The implementation of NTPv4 for VOSS 8.3.100 has the following limitations and requirements.

- The VOSS 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 on page 20.
- 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.

About This Task

The VOSS 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.

Procedure

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).

About This Task

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 VOSS switch). You must configure an authentication key for each NTP server, up to 10.

Procedure

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
   (Press Enter or Return)
   Key: <secret>
   Key: <secret>
   ```

   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 <ip-addr> authentication-key <keyid>
   ```

   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

VOSS 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.

Procedure

1. Access global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Specify the interval.

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

   Valid values range from 4 to 17.

Restrict NTP Traffic

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

Procedure

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.
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.

About This Task

The following examples show typical output for the commands. Your output will vary.

Procedure

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
```

Configure the Domain Name System

Configure DNS for Common Criteria compliance.

Procedure

1. Enter global configuration mode.

```
# enable
# configure terminal
```

2. Configure the host name for the switch.

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

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

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 two examples: one for a DNS host name and one for an IPv4 address.

```
(config)# ping <host-name>
(config)# ping <ipv4-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 VOSS 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.

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

Algorithms that are not approved for use in the Common Criteria configuration are also enabled by default and must be disabled. For more information, see Disable Unapproved Encryption Methods on page 25.

MAC algorithms

Only HMAC-SHA1 and HMAC-SHA2-256 are approved and both are enabled by default. Algorithms that were not evaluated, but are enabled by default, must be disabled. For more information, see Disable Unapproved Authentication Methods on page 26.

Key exchange method

Only the Diffie-Hellman-Group14-SHA1 method is approved and it is enabled by default. No extra configuration is needed or allowed.

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 on page 27, Enable X.509 Authentication on page 28, and Certificate Management on page 30.

Host authentication method

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 on page 26, Enable X.509 Authentication on page 28, and Certificate Management on page 30.

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 SSH Rekeying on page 29.

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.

About This Task

This procedure does not stop or start the SSH service. It merely enables the service in VOSS.

Procedure

1. Enter 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 Unapproved Encryption Methods

You must disable 7 methods that are enabled by default but not allowed in the Common Criteria configuration.

About This Task

Only the following methods are approved and they are enabled by default:

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

Procedure

1. Enter global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Disable SSH.

   ```
   (config)# no ssh
   ```

3. Disabled the unapproved methods.

   ```
   (config)# no ssh encryption-type rijndae128-cbc
   (config)# no ssh encryption-type rijndae256-cbc
   (config)# no ssh encryption-type AES192-CTR
   (config)# no ssh encryption-type AES192-CBC
   (config)# no ssh encryption-type 3DES-CBC
   (config)# no ssh encryption-type Blowfish-CBC
   (config)# no ssh encryption-type aead-aes-192-gcm-ssh
   ```

4. Enable SSH.

   ```
   (config)# ssh
   ```

Disable Unapproved Authentication Methods

You must disable 2 unapproved methods that are enabled by default but not allowed in the Common Criteria configuration.

About This Task

Only HMAC-SHA1 and HMAC-SHA2-256 are approved and they are enabled by default.

Procedure

1. Enter global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Disable SSH.

   ```
   (config)# no ssh
   ```

3. Disabled the unapproved methods.

   ```
   (config)# no ssh authentication-type aead-aes-128-gcm-ssh
   (config)# no ssh authentication-type aead-aes-256-gcm-ssh
   ```

4. Enable SSH.

   ```
   (config)# ssh
   ```

Enable RSA Authentication and Generate the Host Key

RSA is a cryptographic system that provides secure data transmission with a public encryption key and a private decryption key (the host key).

About This Task

You must enable RSA and then generate a host key before the switch can accept incoming SSH connections. Generation of a new key overwrites the previous key.

Procedure

1. Access global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Disable SSH.

   ```
   (config)# no ssh
   ```

3. Enable RSA authentication.

   ```
   (config)# ssh rsa-auth
   ```

4. Generate the host key.

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

   In the evaluated configuration, the only valid value for the key size is 2048.

5. Re-enable SSH.

   ```
   (config)# ssh
   ```

6. To manually delete a host key, take the following steps.

   Although generating a new host key automatically overwrites the existing key, you can manually remove the key if needed.

   a. Disable SSH.

      ```
      (config)# no ssh
      ```

   b. Remove the host key.

      ```
      (config)# no ssh rsa-host-key
      ```

   c. Re-enable SSH.

      ```
      (config)# ssh
      ```

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.

Before You Begin

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

About This Task

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.

Procedure

1. Access global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Use SCP to transfer the public key from the client system to the VSP 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
   Privilege: rsa_key_priv

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

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
   (config)# ssh install-user-key priv public rsa
   ```

Enable X.509 Authentication

You configure X.509 authentication as part of the SSH service.

Procedure

1. Access global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Disable SSH.

   ```
   (config)# no ssh
   ```

3. Remove everything after the @ symbol from the user name in the UPN field.

   Perform this step only if an email address is present in the UPN field of the certificate. For example, if the user name is `admin@test.com`, run this command to remove `@test.com`, so that only `admin` is displayed in the system.

   ```
   (config)# ssh x509-auth username strip-domain
   ```

4. Enable X.509 authentication.

   ```
   (config)# ssh x509-auth enable
   ```

5. Enable OCSP as the revocation checking method.

   ```
   (config)# ssh x509-auth revocation-check-method ocsp
   ```

   OCSP must be enabled in the evaluated configuration. For more information, see Certificate Validation with OCSP on page 32.

6. Enable SSH.

   ```
   (config)# ssh
   ```

What to Do Next

Ensure that the related certificates are added to the system and are ready to be used for authentication. For more information, see Certificate Management on page 30.

Configure SSH Rekeying

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).

About This Task

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.

> Note
> SSH must remain enabled while you configure rekeying.

Procedure

1. Access 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.

Procedure

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

VOSS 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, VOSS 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.

Important

- 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, VSP 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 on page 30.

Reconnect a TLS Session

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

About This Task

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

Procedure

1. Disable the syslog server.

   ```
   # disable syslog
   ```

2. Enable the syslog server.

   ```
   # enable syslog
   ```

Certificate Management

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. VOSS 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.

Digital Certificate Configuration

The process for configuring and managing digital certificates is as follows:

1. Configure the subject parameters.
2. Configure subject alternative names (SAN).
3. Generate a key pair.
4. Install a trusted root certificate.
5. Install a CA certificate.
6. Generate a certificate signing request (CSR).
7. Get the certificate signed.
8. Install the signed certificate.

Certificate Provisioning Methods

VOSS 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 VOSS 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, the VSP performs the following actions:

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

Configure Subject Parameters

Subject parameters identify the switch with parameters such as the name, email, company, department, location, and subject name.

About This Task

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.

Table 6: Required subject parameters (continued)

Parameter	Value
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.
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 on page 28 topic.
Unit	The organizational unit of the subject sending the CSR to the CA. Valid entries range from 0 to 64 characters.

Procedure

1. Access 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 on page 34.

Configure Subject Alternative Names

Use subject alternative names (SANs) to associate such values as email address, IP address, or FQDN with a certificate.

About This Task

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 on page 32. 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.

Table 7: SAN parameters

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.

Procedure

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Configure the SANs for the switch.

```
(config)# certificate subject-alternate-name subject-name VSPSubject dns <FQDN>
(config)# certificate subject-alternate-name subject-name VSPSubject e-mail <email-
addr>
(config)# certificate subject-alternate-name subject-name VSPSubject ip <IPv4-addr>
```

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 on page 32.

Generate the Key Pair

You can generate the private and public key pair for RSA cryptography.

About This Task

By default, VOSS 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`.

Procedure

1. Access global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Generate the key pair.

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

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: 0000000000000001000000010200000000030100010000010 0c953119e
   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.

About This Task

You install a root certificate on the switch.

VOSS accepts certificates in DER (binary) format only.

Procedure

1. Access global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Use SCP to move the certificate file from the CA system to the `/initflash/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.

About This Task

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.

VOSS accepts certificates in DER (binary) format only.

Procedure

1. Access global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Use SCP to move the certificate file from the CA system to the `/initflash/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 VOSS system.

About This Task

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 on page 32, Generate the Key Pair on page 35, and Configure Subject Alternative Names on page 34.

Procedure

1. Access 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 /initflash/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.

What to Do Next

Export the CSR and have it signed.

Sign the Certificate

You use third-party applications to export the CSR, sign the certificate, and import the signed certificate to the VOSS system.

About This Task

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.

Procedure

1. Use SCP to export the CSR from the `/initflash/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 `/initflash/shared/certs` folder.
4. If necessary, convert the signed certificate to DER (binary) format.

   VOSS 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>
   ```

What to Do Next

Install the signed certificate.

Install a Signed Certificate

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

Before You Begin

- Ensure you have imported the signed certificate to the `/initflash/shared/certs` folder. For more information, see Sign the Certificate on page 37.
- 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.

Procedure

1. Access global configuration mode.

   ```
   # enable
   # configure terminal
   ```

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

```
(config) # ls /initflash/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.

Procedure

1. Access 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.

Procedure

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Remove the specified key.

```
(config)# certificate remove key <key-label>
```

Audit Logs and Syslog

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

The VOSS switch can communicate with any syslog server that supports the syslog and TLSv1.2 protocols.

If the connection to the external audit server is lost, the VOSS switch continues to save local audit logs so there is no loss of audit.

If the syslog connection is broken, records that were received by the switch's internal logging service are not forwarded to the external syslog server. These records are skipped.

Log Message Format

The 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.
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 switch. For a remote session, the remote IP address is identified.
User name	Specifies the user name that was used to log in to the switch.
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

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.
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 IPv4 addresses.

Log Files

The VOSS switch captures audit records (such as hardware and software log messages, and alarm messages) into log files. These files are stored in internal flash.

When disk space usage reaches 75% of capacity, the system generates a `disk space 75% full` alarm and the switch stops saving log files to flash. In this scenario, audit records are sent to a connected syslog server, but they are not stored in local internal flash. If no syslog server is connected, audit data is not generated.

To restore auditing and have log files saved, the administrator must free disk space in flash to reduce the disk space usage to below 75%. When disk space usage falls below 75%, the system clears the alarm, and then starts logging to a file again.

Log files have the following naming rules:

- The log file name has 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

As the syslog client, the VOSS switch communicates with an external syslog (audit) server by establishing a trusted channel between itself and the audit server.

About This Task

Implementation of the trusted channel employs port forwarding using Transport Layer Security (TLS v1.2) with X.509 v3 certificate-based authentication between a remote syslog server and the switch. For more information, see Certificate Management on page 30.

Should the connection fail between the syslog server and the switch, attempts to reestablish the connection occur every 2 minutes for up to 2 hours.

The VSP accepts certificates from a syslog server that identify the server with its IPv4 address in the SAN or CN. The VSP also accepts certificates from a syslog server that identify the server with its DNS name in the SAN or CN, as long as that DNS name can be resolved to the IPv4 address in the VSP configuration.

Take the following steps to set up a remote port forwarding connection between the switch and the syslog server that is installed on a host that serves as a TLS server.

Procedure

1. Access global configuration mode.

```
# enable
# configure terminal
```

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

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

   Valid values for the host ID range from 1 to 10 characters. Valid IPv4 addresses are in A.B.C.D format.
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-cert-name <cert-name>
   ```

   Valid values for the certificate name range from 1 to 64 characters and specify the name of the X.509 v3 certificate.
5. Define the TCP port for secure forwarding.

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

   Valid values for the TCP port number range from 1025 to 49151. The default is 1025.

Enable CLI Logging

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

Procedure

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 in the memory buffer by parameters such as file name, category, and severity.

Procedure

1. Access user EXEC mode.

   ```
   # enable
   ```

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

   ```
   # show logging file
   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 logging 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 log entries.

   ```
   # show logging detail
   ```

6. View logs for a specific event code.

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

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

7. View logs for a specific module.

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

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

8. View the logs from a specified file.

   ```
   # show logging name-of-file <string>
   ```

   Valid strings of no more than 99 characters include the path and file name, such as `/intflash/logcopy.txt`.

9. View logs for one or more severity levels.

   ```
   # show logging 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.

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

    ```
    # show logging tail
    ```

Clear Log Messages and Files

You can clear log messages from memory and delete the active log files.

Procedure

1. Access privileged EXEC mode.

   ```
   # enable
   ```

2. Clear the memory file.

   ```
   # clear logging
   ```

3. Delete log files.

   a. Determine which file is the active log file.

   ```
   # show logging info
   Total disk space consumed: 69.21%
   Number of messages lost to log: 0
   Current Log File: /intflash/shared/log.8f800001.129
   ```

   b. Show all log files stored on the system.

   ```
   # ls
   Listing Directory /intflash/shared:
   ```

```
drwxr-xr-x  4 0        0           7336 Oct  6 12:40  ./
drwxr-xr-x 34 0        0           7320 Oct  6 13:16  ../
drwxr-xr-x  2 0        0            504 Jul 18 16:36  certs/
-rwx------  1 0        0           7916 Oct  6 13:16  config.cfg
-rw-r--r--  1 0        0           1421 Jul 18 13:33  interCA.good.cert.der
-rw-------  1 0        0           7396 Feb 14 20:54  log.8f800001.047
-rw-------  1 0        0          12617 Feb 14 20:56  log.8f800001.048
```

Files with names that start with `log` are stored on the system.

c. To delete one log file, run the following command and enter `y` at the prompt.

```
# del <filename>
Remove ./<filename> (y/n) ?
```

d. To delete multiple log files, run the following command.

```
# del log.* -y
```

Wild card characters are supported and **`-y`** answers the prompt with `y`.

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 VOSS 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 Common Criteria Certification Configuration on page 10.

Table 8: Audit record samples

Requirement Identifier	Auditable Event	Audit Record Text
FAU_GEN.1	Start of audit functions	2022-05-27T19:26:54.223Z vsp4900 CP1 - 0x0000065e - 00000003.1 DYNAMIC CLEAR GlobalRouter SW INFO Slot 1: Intflash disk space utilization - below 75%, allow logging to file.
FAU_GEN.1	Stop of audit functions	2022-09-15T20:06:43.456Z vsp4900 CP1 - 0x0000065d - 00000003.1 DYNAMIC SET GlobalRouter SW WARNING Slot 1: Intflash disk space utilization - above 75%, stop logging to file.
FAU_GEN.1	Reset passwords	2022-05-27T18:05:37.958Z vsp4900 CP1 - 0x0000461d - 00000000 GlobalRouter SNMP INFO Admin Password Change success
FCS_NTP_EXT.1	Add time server	2022-02-01T20:47:36.251Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 904 SSH:192.168.144.253 gssadmin ntp server 192.168.144.253 auth-enable
FCS_NTP_EXT.1	Remove time server	2022-09-26T15:50:44.179Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 10 SSH:192.168.144.253 gssadmin no ntp server 192.168.144.2 auth-enable
FCS_SSHS_EXT.1	No matching method	SyslogReceipt:2021-11-19T20:56:28.580077-05:00 Host:vsp4900 AuditTimestamp:2021-11-20T01:56:27.225Z SyslogMessage:CP100000000 GlobalRouter SSH INFO SSH connection negotiation failed. No matching method(s) found for at least one of key exchange, host key, cipher, mac or compression for host 192.168.144.254.

Table 8: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FCS_SSHS_EXT.1	Oversized packet	2022-07-18T18:33:18.147Z vsp4900 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	2022-07-12T22:38:14.901Z vsp4900 CP1 - 0x000d8633 - 00000000 GlobalRouter SSH INFO SSH Server: Rekey initiated because time exceeds 3600 seconds.
FCS_SSHS_EXT.1	Rekey for volume	2022-07-12T18:57:26.575Z 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	2022-07-15T18:06:55.774Z vsp4900 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.
FCS_TLSC_EXT.1	Signature algorithm mismatch	2022-07-15T16:48:30.875Z vsp4900 CP1 - 0x00070618 - 00000000 GlobalRouter SW ERROR TLS handshake between Syslog Client and Server failed with status=ERR_SSL_INVALID_KEY_TYPE.
FCS_TLSC_EXT.1	No matching cipher	2022-07-15T13:38:29.899Z vsp4900 CP1 - 0x00070618 - 00000000 GlobalRouter SW ERROR TLS handshake between Syslog Client and Server failed with status= ERR_SSL_FATAL_ALERT_HANDSHAKE_FAILURE.

Table 8: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FCS_TLSC_EXT.1	Wrong TLS version	2022-07-15T17:52:30.528Z vsp4900 CP1 - 0x00070618 - 00000000 GlobalRouter SW ERROR TLS handshake between Syslog Client and Server failed with status=ERR_SSL_PROTOCOL_VERSION.
FCS_TLSC_EXT.1	Handshake error	2021-12-20T13:47:10.837Z vsp4900 CP1 CP100000000 GlobalRouter SW ERROR TLS handshake between Syslog Client and Server failed with status= ERR_SSL_FATAL_ALERT_HANDSHAKE_FAILURE.
FCS_TLSC_EXT.1	Bad record MAC	2022-02-16T22:10:59.918Z vsp4900 CP1 - 0x00070629 - 00000000 GlobalRouter SW ERROR Fatal alert - SSL_ALERT_BAD_RECORD_MAC detected during TLS negotiation with IP 192.168.144.253.
FIA_AFL.1	Failed login due to exceeding limit	2021-12-20T18:27:59.880Z vsp4900 CP1 CP100000000 GlobalRouter SSH WAR NING Unauthorized login attempt with the user gssadmin and the number of unsuccessful attempts are: 4 and unsuccessful login attempt time is: Mon Dec 20 18:27:59 2021.
FIA_UAU_EXT.2	All use of identification and authentication mechanisms	See FIA_UIA_EXT.1.
FIA_UIA_EXT.1	Successful console login	2022-08-10T13:52:13.135Z vsp4900 CP1 - 0x000305ca - 00000000 GlobalRouter SW INFO user gssadmin connected by console port.
FIA_UIA_EXT.1	Failed console login	022-08-10T13:49:27.518Z vsp4900 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 2022

Table 8: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FIA_UIA_EXT.1	Failed console login	2022-08-10T13:49:27.518Z vsp4900 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:2021-11-19T20:49:37.368157-05:00 Host:vsp4900 AuditTimestamp:2021-11-20T01:49:36.016Z SyslogMessage:CP100000000 GlobalRouter SSH INFO SSH user authentication succeeded for user gssadmin on host 192.168.144.254.
FIA_UIA_EXT.1	Failed SSH/CLI login (Password)	SyslogReceipt:2021-11-19T20:49:51.688973-05:00 Host:vsp4900 AuditTimestamp:2021-11-20T01:49:50.336Z SyslogMessage:CP100000000 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 2021.
FIA_UIA_EXT.1	Failed SSH/CLI login (Password)	SyslogReceipt:2021-11-19T20:49:51.689463-05:00 Host:vsp4900 AuditTimestamp:2021-11-20T01:49:50.336Z SyslogMessage:CP100000000 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)	2022-07-11T20:18:41.605Z vsp4900 CP1 - 0x000d8602 - 00000000 GlobalRouter SSH INFO SSH RSA Public Key authentication succeeded for user operator on host 192.168.144.253.

Table 8: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FIA_UIA_EXT.1	Failed SSH/CLI login (Public Key)	SyslogReceipt:2021-11-19T20:54:36.005444-05:00 Host:vsp4900 AuditTimestamp:2021-11-20T01:54:34.651Z SyslogMessage:CP100000000 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)	2022-08-23T14:21:56.327Z vsp4900 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)	2022-09-14T15:14:47.353Z vsp4900 CP1 - 0x000d8602 - 00000000 GlobalRouter SSH INFO SSH X509 certificate authentication failed for user GssTestUser on host 192.168.144.253.
FIA_X509_EXT.1/Rev	Add trust anchor	2021-12-20T16:24:44.058Z vsp4900 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	2021-12-14T12:06:09.515824-05:00 Host:vsp4900 AuditTimestamp:2021-12-14T17:06:25.845Z 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	2022-07-20T18:18:30.538Z vsp4900 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 8: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FIA_X509_EXT.1/Rev	Invalid EKU	2022-02-16T19:30:59.504Z vsp4900 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)	2022-10-27T13:31:20.595Z vsp4900 CP1 - 0x003a8675 - 00000000 GlobalRouter DIGITALCERT ERROR Invalid Certificate! Details = [Invalid Basic Constraints] 2022-10-27T13:31:20.595Z vsp4900 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)".
FIA_X509_EXT.1/Rev	Basic constraints missing for CA (Syslog)	2022-07-22T16:48:30.536Z vsp4900 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 2022-07-20T15:38:30.654Z vsp4900 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	2021-12-20T14:51:37.937Z vsp4900 CP1 CP100000000 GlobalRouter SW ERROR Fatal alert - SSL_ALERT_CERTIFICATE_EXPIRED detected during TLS negotiation with IP 192.168.144.253.

Table 8: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FMT_MOF.1/Manual Update	Manual update attempts (trusted update)	2022-02-03T21:17:26.936Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 202 CONSOLE gssadmin software add VOSS4900.8.3.100.0int083.tgz 2022-02-16T04:26:02.768Z vsp4900 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	2021-12-21T14:28:26.006Z vsp4900 CP1 - 0x0003064a - 00000000 GlobalRouter SW INFO Clock set successfully. New time:Tue Dec 21 14:28:26 2021 UTC, Prev time: Sat Nov 11 11:11:14 2000 UTC,Initiated by SSH, user: gssadmin from IP: 192.168.144.253.
FPT_TUD_EXT.1	Software signature verification failed	2022-08-25T14:42:07.818Z vsp4900 CP1 - 0x00264511 - 00000000 GlobalRouter SW INFO Image signature verification FAILED user gssadmin.
FTA_SSL.3	Remote session termination	2022-01-03T20:40:15.282Z vsp4900 CP1 - 0x0003067a - 00000000 GlobalRouter SW INFO User gssadmin forced log-out after CLI session inactivity of 180 seconds.
FTA_SSL.4	SSH logout	2022-09-15T16:13:22.718Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 433 SSH: 192.168.144.253 gssadmin logout.
FTA_SSL.4	Console logout	2022-01-03T20:40:24.090Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 486 CONSOLE gssadmin logout.

Table 8: Audit record samples (continued)

Requirement Identifier	Auditable Event	Audit Record Text
FTA_SSL_EXT.1	Forced lockout after CLI inactivity	2022-09-23T14:08:13.454Z 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	2021-12-20T13:49:48.587Z vsp4900 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	2021-12-20T13:47:57.318Z vsp4900 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:2021-11-19T20:49:37.868114-05:00 Host:vsp4900 AuditTimestamp: 2021-11-20T01:49:36.018Z SyslogMessage: CP100000000 GlobalRouter SSH INFO SSH CLI session start: user gssadmin on host 192.168.144.254.
FTP_TRP.1/Admin	SSH session termination	SyslogReceipt:2021-11-19T20:49:38.875016-05:00 Host:vsp4900 AuditTimestamp: 2021-11-20T01:49:37.371Z SyslogMessage: CP100000000 GlobalRouter SSH INFO SSH CLI session end: user gssadmin on host 192.168.144.254.
FTP_TRP.1/Admin	SSH session termination	SyslogReceipt:2021-11-19T20:49:38.875939-05:00 Host:vsp4900 AuditTimestamp: 2021-11-20T01:49:37.371Z 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 VOSS switch.

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.

Table 9: Administrative action records

Admin Action	Scenario or Command	Audit Record Text
Log-in	Connected through console port	2021-12-20T13:39:40.588Z vsp4900 CP1 CP100000000 GlobalRouter SW INFO user gssadmin connected through console port
Log-in	Logged in	2022-01-07T13:34:21.144206-05:00 Host:vsp4900 AuditTimestamp :2022-01-07T18:34:20.277Z 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 2022
Log out	Logged out from console port	2021-12-21T20:15:20.840Z vsp4900 CP1 - 0x00030637 - 00000000 GlobalRouter SW INFO user gssadmin logged out from console port
Log out	SSH CLI session end	2022-01-07T13:34:28.970645-05:00 Host:vsp4900 AuditTimestamp :2022-01-07T18:34:27.744Z SyslogMessage:CP100000000 GlobalRouter SSH INFO SSH CLI session end: user gssadmin on host 192.168.144.253
Configure SSH rekey (volume)	ssh rekey data-limit	2022-07-11T18:59:33.168Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 1380 CONSOLE gssadmin ssh rekey data-limit 1
Configure SSH rekey (time)	ssh rekey time-interval	2022-07-11T18:59:04.183Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 1377 CONSOLE gssadmin ssh rekey time-interval 1
NTP server config	Enable NTP server	2022-02-01T20:47:36.251Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 904 SSH:192.168.144.253 gssadmin ntp server 192.168.144.253 auth-enable
NTP server config	Disable NTP server	2022-09-26T15:50:44.179Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 10 SSH:192.168.144.253 gssadmin no ntp server 192.168.1 44.2 auth-enable
Manually specify clock value	set clock	2021-12-21T14:28:26.006Z vsp4900 CP1 - 0x0003064a - 00000000 GlobalRouter SW INFO Clock set successfully. New time:Tue Dec 21 14:28:26 2021 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	2022-02-03T21:17:26.936Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 202 CONSOLE gssadmin software add VOSS4900.8.3.100.0in t083.tgz

Table 9: Administrative action records (continued)

Admin Action	Scenario or Command	Audit Record Text
Trusted update	software activate	2022-02-16T04:26:02.768Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 4 CONSOLE gssadmin software activate VOSS4900.8.3.10 0.0int089
Set timeout value	Set CLI timeout	2022-09-15T16:13:19.705Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 428 SSH:192.168.144.253 gssadmin cli timeout 7200
Ability to configure the access banner	banner custom	2022-05-28T20:18:48.328Z vsp4900 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	2021-12-23T14:34:13.128Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 117 SSH:192.168.144.253 gssadmin ssh timeout 60
Ability to update the system, and to verify the updates using [digital signature] capability before installing those updates	Image signature verification FAILED	2022-08-16T17:25:27.898Z vsp4900 CP1 - 0x00264511 - 00000000 GlobalRouter SW INFO Image signature verification FAILED
Ability to configure the authentication failure parameters for FIA_AFL.1	default-lockout-retries	2021-12-21T19:19:58.467Z vsp4900 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	2022-01-07T13:41:33.436018-05:00 Host:vsp4900 AuditTimestamp :2022-01-07T18:41:32.567Z SyslogMessage:CP100000000 GlobalRouter CLILOG INFO 1033 SSH:192.168.144.253 gssadmin syslog host 1 enable
Ability to manage the cryptographic keys	generate-keypair	2022-08-16T18:38:12.779Z vsp4900 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	2022-02-09T21:07:13.864Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 105 SSH:192.168.144.253 gssadmin ssh x509v3-auth enable
Ability to configure NTP	ntp enable	2021-12-22T17:24:01.811Z vsp4900 CP1 - 0x000c8587 - 00000000 GlobalRouter SW INFO NTP Enabled
Ability to manage the system's trust store and designate X509.v3 certificates as trust anchors,	ssh x509v3-auth ca-name	2022-09-23T17:28:34.954Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 771 SSH:192.168.144.253 gssadmin ssh x509v3-auth ca-na me Global

Table 9: Administrative action records (continued)

Admin Action	Scenario or Command	Audit Record Text
Ability to import X509 v3 certificates to the system's trust store	certificate install-file offline-ca-filename	2022-09-23T17:48:47.608Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 775 SSH:192.168.144.253 gssadmin certificate install-file offline-ca-filename subca-rsa.der
Ability to manage the trusted public keys database	ssh install-user-key	2022-11-18T01:37:36.119Z vsp4900 CP1 - 0x002c0600 - 00000000 GlobalRouter CLILOG INFO 1939 CONSOLE gssadmin ssh install-user-key operator public rsa

General Configuration Tasks

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.

Procedure

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

The banner messages provide information to users who access the VOSS command-line interface over a serial connection or an SSHv2 connection.

About This Task

You can configure the message that users see before they log in (called a custom banner) and the message of the day (MOTD), which they see after they log in.

Procedure

1. Access global configuration mode.

```
# enable
# configure terminal
```

2. Enable the switch to use a custom banner.

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

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

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

   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. Each line of message text can support up to 80 characters. The total number of characters in the message cannot exceed 1896 characters.

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

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

   To create a MOTD with multiple lines, use the **banner motd** command before each new line of the message. To create a string of words separated by spaces, surround the text in quotation marks. Each line of message text can support up to 80 characters. The total number of characters in the MOTD cannot exceed 1516 characters.

5. Enable the message of the day.

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

6. Save your messages.

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

7. Verify your messages.

   ```
   (config)# show banner
   ```

8. Stop and start the internal SSH server.

   This step allows the banner and the MOTD to display when users access VOSS over an SSHv2 connection.

   ```
   (config)# no ssh
   (config)# ssh
   ```

Example

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. Log out now."

```
# enable
# configure terminal
(config)# banner custom
(config)# banner Company
(config)# banner www.Companyname.com
(config)# banner motd "Unauthorized access to this system is forbidden."
(config)# banner motd "Log out now."
(config)# banner displaymotd
(config)# save config
(config)# no ssh
(config)# ssh
```

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.

About This Task

If inactivity exceeds that threshold, the session is disconnected and the user must log in again.

Procedure

1. Access 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

The VSP performs software upgrades using what the Protection Profile calls a "delayed activation" method.

The software is installed in the software inventory before being activated. When you activate the upgrade image, the new software becomes the primary image. The current primary image becomes the backup image. The current backup image becomes an available image in the inventory. You are prompted to reset the switch to complete the activation process.

The process of upgrading VOSS involves the following tasks.

Software inventory

> You can verify the running version of the software anytime by using the **show software** command. For more information, see Display Software Inventory on page 58.

Configuration backup

> You back up the configuration so that the switch can reapply the configuration after it is restarted. For more information, see Back Up the Configuration on page 59.

Image download

> You download the upgrade image (*.tgz) file to a location that the switch can access. For more information, see Download the Upgrade Image on page 59.

Software upgrade

> With the delayed activation method, the current version of the software continues to run until you reset the switch to complete the activation. For more information, see Upgrade the Software on page 60

Display Software Inventory

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

Procedure

1. Access privileged EXEC mode.

   ```
   # enable
   ```

2. Verify the running version of the software.

   ```
   # show software
   ```

Example

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 2022 EDT
************************************************************
software releases in /intflash/release/
************************************************************
5520.8.3.100.0int097 (Signed Release)
5520.8.3.100.0int098 (Backup Release (Signed Release)
5520.8.3.100.0int112 (Primary Release) (Signed Release)

------------------------------------------------------------
Auto Commit     : enabled
Commit Timeout  : 10 minutes
```

Back Up the Configuration

When you back up the configuration, the switch can reapply the configuration after the software is upgraded and the switch is restarted.

Procedure

1. Enter Privileged EXEC mode.

   ```
   # enable
   ```

2. Determine the name of the configuration file.

   ```
   # show boot config choice
   ```

   The command returns results similar to the following example, in which there is a primary configuration file and a backup configuration file.

   ```
   choice primary config-file "/intflash/config.cfg"
   choice primary backup-config-file "/intflash/config.cfg"
   ```

3. Save the configuration file.

   ```
   # save config file <file-name>
   ```

4. Copy the configuration file to a location that is accessible from the switch.

   ```
   # copy /intflash/config.cfg <ip-addr>/dir/config_backup.cfg
   ```

Download the Upgrade Image

The upgrade image (*.tgz) file contains the executable code that runs on the switch.

Procedure

1. Obtain the upgrade image from the Extreme Networks support site: http://www.extremenetworks.com/support.

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

2. Use SCP or an SFTP client to place the image files in the following location on a server that your switch can locate: `/initflash/shared`.

Upgrade the Software

This procedure shows how to upgrade the software using the internal flash memory as the file storage location.

About This Task

During upgrade, the system verifies the digital signatures that are embedded in the upgrade files and rejects installation of an image that has an invalid signature.

Procedure

1. Access global configuration mode.

   ```
   # enable
   # configure terminal
   ```

2. Transfer the upgrade files to the switch using SCP or through the USB port.
3. Extract the upgrade files.

   ```
   (config)# software add <version>
   ```

   The image files are added to the software image storage subsystem and the files are extracted to the `/intflash/release` directory, as shown in the following example.

   ```
   (config)# software add 5520.8.3.100
   Extracting distribution information from /intflash/shared/5520.8.3.100.0int116.voss
   Checking signature of file /intflash/shared/5520.8.3.100.0int116.voss
   Image signature verification PASSED.
   Extracting software version 5520.8.3.100.0int116 from /intflash/shared/
   5520.8.3.100.0int116.voss
   Extraction of 5520.8.3.100.0int116 to /intflash/release/5520.8.3.100.0int116 successful
   Setting permissions on /intflash/release/5520.8.3.100.0int116 successful
   ```

4. Display the software inventory to confirm that the image files were added.

   ```
   (config)# show software
   ```

   See Display Software Inventory on page 58 for sample output.

5. Activate the upgrade image, which copies the specified version to the boot flash file.

   ```
   (config)# software activate <version>
   ```

   The activated software becomes the primary image. The current primary image becomes the backup image. The current backup image becomes an available image in the inventory. You are prompted to reset the switch to complete the activation.

6. At the prompt to reset the switch, enter `y`.

   The activation process is completed, the system restarts, the new release is installed, and system parameters are loaded. The parameters come from the most recent configuration file.

7. Access privileged EXEC mode.

   ```
   # enable
   ```

8. Verify that the software release is installed.

   ```
   # show software
   ```

   Command output shows the software inventory on the system, including primary and backup versions. See Display Software Inventory on page 58 for sample output.

9. Commit the new software, which ensures that the software release is trusted.

```
# software commit
```

Tip
The software is automatically committed 10 minutes after the system is restarted and the software installed (step 6).

Example

The following is an example of output from the **`software add`** command when the image is unsigned.

```
(config)# software add VOSS8400.073_Unsigned.tgz
Extracting distribution information from /intflash/shared/VOSS8400.073_Unsigned.tgz
ERROR: While running in Enhanced Secure Mode only signed software
     images can be loaded on the switch!
```

Example

The following is an example of output from the **`software add`** command when the image is corrupted.

```
(config)# software add VOSS8400.072_wrongkey.tgz
Extracting distribution information from /intflash/shared/VOSS8400.072_wrongkey.tgz
Checking signature of file /intflash/shared/VOSS8400.072_wrongkey.tgz
ERROR : Software signature verification FAILED!
This can be due to archive corruption or tampering with the file.

# 1 2022-09-28T11:03:51.552+00:00 VSP-8404 CP1 - 0x00264511 -
     00000000 GlobalRouter SW INFO Image signature verification FAILED user adminuser
```

Example

The following is an example of output when the **`software activate`** command is successful.

```
(config)# software activate VOSS8400.8.3.100.0int111
Executing software activate for version VOSS8400.8.3.100.0int111.
Validating release VOSS8400.8.3.100.0int111
[09/28/22 11:15:13] Sending upgrade message to slots: 1. Version=VOSS8400.8.3.100.0int111
[09/28/22 11:15:20] Slot 1 : IMAGE SYNC: Running pre-install script for image
     version VOSS8400.8.3.100.0int111
[09/28/22 11:15:21] Slot 1 : IMAGE SYNC: uBoot image is consistent
[09/28/22 11:15:21] Slot 1 : IMAGE SYNC: Kernel image is consistent
[09/28/22 11:15:21] Slot 1 : IMAGE SYNC: Root_FS image is consistent
[09/28/22 11:15:21] Slot 1 : IMAGE SYNC: APP_FS image is being updated...
1 2022-09-28T11:16:12.368+00:00 VSP-8404 IO1 - 0x00264541 - 00000000 GlobalRouter SW INFO
     Image Integrity verification passed.
[09/28/22 11:16:14] Slot 1 : IMAGE SYNC: Running post-install script for image version
     VOSS8400.8.3.100.0int111
[09/28/22 11:16:14] Slot 1 : IMAGE SYNC: Backup image successfully upgraded to
     VOSS8400.8.3.100.0int111

Primary Version:   VOSS8400.8.3.100.0int111
Backup Version:    schiriac-cert-exp1

Changes will take effect on next reboot.
It is strongly recommended to reset the switch after this upgrade.
     Do you want to reset the switch now? (y/n) ?
```