


## HPE 8360v2 Switch Series



# HPE 8360v2 Switch Series User Guide

[Home](#) » [HPE](#) » HPE 8360v2 Switch Series User Guide 

### Contents

- [1 HPE 8360v2 Switch Series](#)
- [2 Introduction](#)
- [3 Software Signing and Verification](#)
- [4 Management Interfaces](#)
- [5 Web Interface](#)
- [6 Configuring Login Banner](#)
- [7 Finalizing Configuration](#)
- [8 Audit Functionality](#)
- [9 Self Tests](#)
- [10 Key Destruction](#)
- [11 Documents / Resources](#)
  - [11.1 References](#)

# HPE

## HPE 8360v2 Switch Series



## Introduction

### Purpose

This document serves as a supplement to the official Aruba User Documentation, consolidating configuration information specific to the Common Criteria Protection Profile requirements. This guide provides the information an administrator would need to set up and administer the Aruba Switch Series network appliances in compliance

with the Common Criteria evaluated configuration. Follow this guide in its entirety to ensure that the settings of each parameter meet the specific configuration that was evaluated and certified as secure by the Common Criteria certification.

**Intended Audience**

- This information is intended for use by administrators who are responsible for investigating and managing network security for their organization.
- To use this guide, you must know your organization's network infrastructure and networking technologies.

**Evaluated Configuration**

- This document covers the Aruba 4100, 6000, 8000, 9000, and 10000 Switch Series running version 10.11, which was evaluated the NDcPP requirements.
- The evaluation of the Aruba 4100, 6000, 8000, 9000, and 10000 Switch Series covered specific items such as auditing, identification and authentication, and remote management using SSH.
- While the physical form factor of each appliance in the Aruba Campus Switch Series may vary, the underlying hardware and software share a similar architecture.
- The software utilizes a common code base of a modular nature with only the modules applicable for the specific hardware loaded.

**Assumptions**

There are specific conditions that are assumed to exist in the HPE Switches for Operational Environment. The following table lists assumptions about the Operational Environment.

**TABLE 1 – ASSUMPTIONS**

Assumptions for Operational Environment	
No General Purpose	It is assumed that general-purpose computing capabilities are not used for any other purpose but as required for the operation, administration and support of the device.
Physical Security	The physical security, commensurate with the value of the device and the data it contains, is assumed to be provided by the operational environment.
Administration	All administrators are trusted to follow and apply all guidance in a secure and trusted manner.

**Setting up Common Criteria Configuration**

In the factory default configuration, the switch has no IP (Internet Protocol) address or subnet mask, and no password set. This section will describe the steps required to configure the switch in accordance with the security objectives in the Security Target, including:

- IP address configuration
- User and password management
- Date and time configuration
- Cryptographic functionality

## Connecting through the Console Port or Management Port

### Connecting to the Console Port

The Console Port must be used to create a physically protected administrative interface that is local to the switch(s) being managed. While access to this interface is protected by the login process, actions at the local console can prevent a switch from booting into an evaluated configuration. Additionally, the switch does not lock administrative access through local console as a result of failed logins. Therefore, it is necessary to provide physical protection of the switch local console to ensure the boot process and avoid unlimited password guesses on the administrator accounts. The switch and its local console should be protected using equivalent physical security.

#### Procedure:

1. Connect the console port on the switch to the serial port on the management station using a console cable.
2. Start the terminal emulation software on the computer and configure a new serial session with the following settings:
  - Speed: 115200 bps
  - Data bits: 8
  - Stop bits: 1
  - Parity: None
  - Flow control: None
3. Start the terminal emulation session.
4. Press Enter once. If the connection is successful, you are prompted to login.

### Connecting to the Management Port

#### Procedure:

1. Use an Ethernet cable to connect the management port to your network. By default, the management port is set to operate as a DHCP client. Retrieve the IP address assigned to the port from your DHCP server.
2. Use an Ethernet cable to connect your computer to the same network.
3. Start your SSH client software and configure a new session using the address assigned to the management port.
4. Start the session. If the connection is successful, you are prompted to login.

### Use of the CLI

When configuring the switch through the CLI, the operator must be working with Administrator role privileges. A CLI prompt with Administrator role privileges will have a “#” at the end, as in the following example:

- switch#

Additionally, the operator must be in the Configuration context before issuing CLI configuration commands. A CLI prompt with Administrator role privileges in Configuration context will have a (config)# at the end, as in the following example:

- switch(config)#

Before configuring the switch via the CLI, the operator must issue the following command to enter the Configuration context:

- switch# configure

To exit the Configuration context, enter the exit command.

**Example:**

- switch(config-vlan-100)# exit
- switch(config)#

### **IP Address Configuration**

By default, the switch is configured to automatically receive IP addresses from a DHCP server that has been configured correctly with information to support the switch. In the evaluated configuration, the switch should be restricted to communicating from a static IP address on a known, isolated port. This section will walk through the following configurations.

### **Virtual routing and forwarding**

The term “vrf” (Virtual Routing and Forwarding) is used throughout this configuration guide. A VRF is a virtual instance of the routing stack and a way to segment the switch into multiple segments. This guide provides instructions on how to setup the switch over the out-of-band management (OOBM) interface which is denoted by the term “mgmt”.

### **Disabling Central Client**

With Aruba Central out-of-scope of the evaluated configuration, the Aruba Central client on the switches should be disabled with the following commands:

- switch# configure
- switch(config)# Aruba-central
- switch(config-Aruba-central)# disable

### **Updating Switch Software**

- Prior to beginning evaluation, the operator must download the validated firmware image from HPE and load it onto the switch using the update methods either using SFTP or USB listed in the following section.
- Please visit the CCEVS Product Compliant List ( <https://www.niap-ccevs.org/Product/>) for the validated version of the product software to use.
- To avoid damage to your equipment, do not interrupt power to the switch during a software update. HPE does not recommend performing any configuration changes until all upgrades are completed.

### **Prerequisites**

- Prior to updating the switch, make sure the management port is connected and configured to use a static IP address.

### **Setup Management Port with a Static IP address**

**Procedure:**

1. Enter the interface mgmt command.  
switch(config)# interface mgmt
2. Enter the ip command.

```
switch(config)# ip static <ip_address> <subnet_mask>
```

3. Enter the no shutdown command.

```
switch(config-if-mgmt)# no shutdown
```

4. Exit the interface mgmt context.

```
switch(config-if-mgmt)# exit
```

### File Transfer setup

For some situations, you may want to use a secure method to issue commands or copy files to the switch. SFTP can provide a secure alternative to TFTP for transferring information that may be sensitive (like switch configuration files) to and from the switch.

### SFTP

Before using SFTP to transfer the software to the switch, make sure:

- A software version for the switch has been stored on a computer accessible to the switch via a management port. (The software file is typically available from the Switch Networking website at <http://www.hpe.com/networking/support>.)
- The switch is properly connected to your network via the management port and has already been configured with a compatible IP address and subnet mask.
- The computer containing the software image is accessible to the switch via IP. Before you proceed, complete the following:
  - Obtain the IP address of the computer on which the software file has been stored.
- Determine the name of the software file stored on the computer for the switch (for example, ArubaOS-CX\_8320\_10\_03\_0001.swi.)

### USB

Before using USB to transfer software to the switch, make sure to:

- The USB flash drive must be formatted with a FAT file system.
- Store a software version on a USB flash drive.
- Insert the USB device into the switch's USB port.
- Determine the name of the software file stored on the USB flash drive.

### Enable USB on the switch:

- switch(config)# usb
- switch(config)# usb mount
- switch(config)# show usb
- Enabled: Yes
- Mounted: Yes

### Copying the software and rebooting the switch

#### Procedure:

1. Copy the software to the secondary flash on the switch using copy command.
  - For SFTP:

```
switch# copy sftp://user@10.0.9.50/ArubaOS-CX_8320_10.02.0020.swi secondary vrf mgmt
```

- For USB:

```
switch# copy usb:/ ArubaOS-CX_8320_10.02.0020.swi secondary
```

2. Select [y] to continue when prompted for the secondary image to be deleted.

3. When the switch finishes downloading the software file, it displays this progress message:

```
Verifying and writing system firmware...
```

```
Success
```

If the software validation fails, the command line will output:

```
Verifying and writing system firmware...
```

```
Verification failed.
```

4. When the installation finishes, confirm the version and the file saved to disk are what was transferred.

```
switch# show images
```

5. You must reboot the switch to implement the newly downloaded software image using the boot system command.

```
switch# boot system secondary
```

6. Upon successful reboot, execute the show version command and verify the correct firmware revision.

```
switch# show version
```

If using a USB, remove the USB drive, as it is no longer needed.

```
switch# usb unmount
```

## Software Signing and Verification

- Aruba has implemented digital signature validation for software versions compatible with the Switch Series. Digitally signed software ensures that the software originated from Aruba and has not been altered.
- The operator will execute the following steps to verify that the software under test has been correctly installed on the switch.

## Flash Verification

- Issue the following command to verify the software version installed to secondary flash:  

```
switch# show images
```
- Displays version information for software images installed to primary and secondary flash
- The switch will display a listing of software images in primary and secondary flash, similar to the following:

---

#### ArubaOS-CX Primary Image

---

Version : TL.10.02.0011D

Size : 351 MB

Date : 2019-02-05 04:13:50 PST

SHA-256 : 1932d9446dff46d062d540c189a5f08e064c5b740d3d13bfb76f1dee56cf5185

---

#### ArubaOS-CX Secondary Image

---

Version : TL.10.02.0020M

Size : 351 MB

Date : 2019-02-20 23:54:30 PST

SHA-256 : 07a9015d6c107a44efa27bc7dc9307f6420b2a2bdbf4c73bd2861a429fb17a4e

---

Default Image : secondary

---

Management Module 1/1 (Active)

---

Active Image : secondary

Service OS Version : TL.01.03.0007-internal

BIOS Version : TL-01-0013

Verify that the version number for the Secondary Image matches the version installed.

### Running Version Verification

- Issue the following command to verify the version of the software currently running on the switch:
  - switch# show version
- Confirm that the version displayed matches the version installed, as indicated by the show images command.

### Firmware Validation

- All Aruba switch firmware is signed by HPE at the time the firmware is created.
- The firmware signature is verified at the time of download and also verified at every boot.
- The public keys used to verify the firmware is stored within the bootloader and firmware.

### Enabling enhanced secure mode

To satisfy the evaluated configuration, the switch must be placed into Enhanced secure mode.

#### Procedure:

1. Reboot the switch into ServiceOS
  - switch# boot system service

Note: On the Aruba 8400 and 6400 switch with two MMs, boot both MMs to ServiceOS first, and then execute the steps on each MM.

2. At the switch login prompt, log in as an admin user account
  - ServiceOS login: admin SVOS>
3. Set the password for the admin using the rules listed below in the User, Password and Session Management section. By default, the admin user does not have a password set.
  - SVOS> password
  - Enter password: \*\*\*\*\*
  - Confirm password: \*\*\*\*\*
4. Enable secure mode
  - switch(config)# secure-mode enhanced
  - Enter [y] for confirmation
5. Wait for reboot and zeroization to complete
6. The device will boot automatically

### **User, Password, and Session Management**

To view or change configuration settings on the switch, users must log in with a valid account. Two types of user accounts are supported:

- Operators: Operators can view configuration settings, but cannot change them. No operator accounts are created by default.
- Administrators: Administrators can view and change configuration settings. A default locally stored administrator account is created with a username set to admin and no password. You set the administrator account password as part of the initial configuration procedure for the switch.

### **General password rules:**

User names and passwords are case-sensitive. ASCII characters in the range of 33-126 are valid, including:

- A through Z uppercase characters
- a through z lowercase characters
- 0 through 9 numeric characters
- Special characters: ! # \$ % & ' ( ) \* + - . / : ; < = > ? @ [ \ ] ^ \_ ` | ~
- The password length ranges from 1 to 32 characters.

Below are a set of rules for constructing strong passwords:

- The passwords should be a combination of alphanumeric characters with lower case characters, upper case characters, and special characters.
- Do not use known information about yourself (e.g. pet names, your name, family names or any information available in the public domain).
- Passwords should be significantly different from previous passwords (adding a '1' or "!" to the end of the password is not sufficient).
- Do not include a complete word with your passwords. (Ex: Password!).

### **Set minimum password length:**



By default, the minimum password length cannot be empty. The user must set the minimum password.

- switch(config)# password complexity
- switch(config-pwd-cplx)# minimum-length <length>
- switch(config-pwd-cplx)# enable

Whenever the minimum password length is set or changed, the admin should ensure that all users change their disqualified passwords.

### Login Management

A user reaching the specified number of failed login attempts will be locked out for the specified length of time before being able to try again. By default, there is no limit of login attempts and no lockout enforcement. This step must be done to establish the limit and lockout. This feature locks out users with SSH but does not lock the console session.

- switch(config)# aaa authentication limit-login-attempts <max-login-attempts> lockout-time <seconds>

### Protecting Credentials

- The user name and password information are saved in encrypted form within the switch.

### Session Timeout

- You can set the session inactivity timeout to a desired value. The default setting is 30 seconds.
  - switch(config)# session-time <value>
- Issue the following command to terminate the local or remote session:
  - switch# exit

**NOTE:** The actual termination may take 5-20 seconds longer than the configured value, administrators should set this value accordingly.

### Date and Time Configuration

- In order to guarantee accurate timestamps in the audit log, the operator must update the date and time on the switch.

### Updating Date and Time Manually

- Issue the following command to manually set the date and time on the switch:
  - switch(config)# clock datetime YYYY-MM-DD HH:MM:SS

### Example:

- This example sets the date and time to December 12, 2017 at 2:15pm.
  - switch(config)# clock datetime 2017-12-12 14:15:00
- To ensure valid timestamps, the switch must be configured with the proper time zone. Issue the following command to configure the switch for the current time zone:

- switch(config)# clock timezone <time-zone>
- For the <time-zone> use a name defined in the IANA time zone database. See [https://en.wikipedia.org/wiki/List\\_of\\_tz\\_database\\_time\\_zones](https://en.wikipedia.org/wiki/List_of_tz_database_time_zones).

#### **Example:**

- To configure the switch for Eastern Standard Time (UTC-5:00), issue the following command:
  - switch(config)# clock timezone EST
- For Greenwich Mean Time (UTC+0:00), issue the following command:
  - switch(config)# clock timezone GMT

#### **Updating Date and Time through NTP**

- While the use of NTP is supported, it is not claimed nor tested in the evaluated configuration.

#### **Management Interfaces**

- The user can log in to the switch using the management interfaces SSH or Console.
- The user should restart the session when the session gets disconnected unintentionally.

##### **Console**

In the factory default configuration, the switch has no static IP (Internet Protocol) address and subnet mask, and no passwords. In this state, it can be managed only through a direct console connection. To manage the switch through in-band (networked) access, the switch must be configured with an IP address and subnet mask compatible with the network accessed. Also, configure an Administrator's and operator's username and passwords to control access privileges from the console and other management interfaces. To log out of the session, the user should execute the "exit" command.

##### **SSH**

- In the evaluated configuration, SSH is enabled by default on the 'mgmt' VRF through the OOBM interface.
- The command "show ssh vrf mgmt" can be used to view the current status of the SSH on 'mgmt' VRF:

```
switch# show ssh server vrf mgmt
```

SSH server configuration on VRF mgmt:

IP Version	: IPv4 and IPv6	SSH Version	: 2.0
TCP Port	: 22	Grace Timeout (sec)	: 60
Max Auth Attempts	: 6	Server status	: running

Ciphers:

aes128-ctr, aes192-ctr, aes256-ctr

Host Key Algorithms:

ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521,  
rsa-sha2-256, rsa-sha2-512

Key Exchange Algorithms:

ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521

MACs:

hmac-sha2-256, hmac-sha2-512

Public Key Algorithms:

rsa-sha2-256, rsa-sha2-512, ecdh-sha2-nistp256, ecdh-sha2-nistp384,  
ecdh-sha2-nistp521

### Command to log out of the SSH session:

- switch# exit

### SSH Rekey

The SSH server will perform a rekey operation for all open SSH sessions at every hour or before 1 GB of data is transferred, whichever occurs first. This is performed to address a common security concern that encryption/decryption keys not be used for long periods. This limits the amount of data exposed in the unfortunate case where a key is exposed/refactored.

### SSH host key generation

- The SSH host key is used by clients to ensure that the server that they're connecting to hasn't changed. There may be times when a host key needs to be regenerated. This can be performed with the following command:
  - switch(config)# ssh host-key [ecdsa [ecdsa-sha2-nistp256 |
  - ecdsa-sha2-nistp384 |
  - ecdsa-sha2-nistp521]]
- When a host key is generated, it overwrites the current key of the same type. To view a generated host key, the administrator can enter the following command:
- Switch# shows ssh host-key

- Should the Security Administrator wish to clear the SSH host keys used by the switch they must zeroize all keys on the switch (including x.509 certificate private keys) using the following command:
  - `switch(config)# erase all zeroize`

## SSH authorized keys

- The switch's SSH server can be configured with a set of SSH public keys that administrators can use for public key authentication. Public keys are associated with local user accounts and can be added with the following:
  - `switch(config)# user <username> authorized-key <authorized_key>`
- SSH public key authentication is enabled by default but can be disabled with the following command:
  - `switch(config)# no ssh public-key-authentication`
- SSH-authorized keys are not saved to persistent storage until the "write memory" or the running configuration is saved.

## Disabling Unsupported Algorithms

In order to comply with the evaluated configuration, the switch must restrict remote SSH connections to only use certified algorithms. Issue the following commands to restrict the set of algorithms used:

```
switch(config)# ssh ciphers aes128-ctr, aes256-ctr, aes128-cbc, aes256-cbc
```

```
switch(config)# ssh macs hmac-sha2-256, hmac-sha2-512, hmac-sha1
```

```
switch(config)# ssh key-exchange-algorithms ecdh-sha2-nistp256, ecdh-sha2-nistp384, diffie-hellman-group14-sha1
```

```
switch(config)# ssh host-key-algorithms ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521
```

```
switch(config)# ssh public-key-algorithms ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521
```

- Individual algorithms are ordered and advertised to the peer SSH device as configured. Please order the algorithms appropriately to ensure that the desired preference of algorithms.

## Certificate Installation and Validation

X.509 digital certificates are used by the Secure Remote Logging feature and allow the switch to present its identity to the remote server as well as validate the identity of the server. The syslog standard mandates the use of mutual authentication which requires the addition of the syslog server's certificate authority and the installation of an end entity certificate for the device.

### 1. Configure the CA certificate of the remote syslog server's PKI:

- `switch(config)# crypto pki ta-profile <TA-NAME> switch(config-ta-cert)# ta-certificate import terminal`
- << paste in the CA certificate of the remote syslog server >>

### 2. Generate a CSR for the syslog client:

- `switch(config)# crypto pki certificate <cert-name>`
- `switch(config-cert-name)# subject [common-name <COMMON-NAME>] [country <COUNTRY>] [locality <LOCALITY>] [org <ORG-NAME>] [org-unit <ORG-UNIT>] [state <STATE>]`
- `switch(config-cert-name)# key-type {rsa [keysize <K-SIZE>] | ecdsa [curve-size <C-SIZE>]}`

- switch(config-cert-name)# enroll terminal
- << dumps the CSR >>

3. Import the signed certificate for the syslog client:

- switch(config-cert-name)# import terminal ta-profile <ta-name> << paste in signed cert >>

When the switch receives a certificate chain from a peer device, it shall validate the following:

1. Verifies the validity dates of all certificates within the chain.
2. Performs a cryptographic path check to ensure that it leads up to a trusted CA certificate installed on the switch.
3. OCSP is used to verify that the EE and CA certificates have not been revoked.
4. Verifies the presence of the Server Authentication purpose bit is set within the extended key usage extension when the peer device is acting as a server.
5. Verifies the presence of the Client Authentication purpose bit is set within the extended key usage extension when the peer device is acting as a client.
6. Verifies the presence of the OCSP Signing purpose bit is set within the extended key usage extension when the peer device is acting as an OCSP responder.
7. Verifies the presence of a SAN in the certificate, or a CN if there is no SAN. The SAN or CN is compared to the value configured by the Security Administrator and may be either a hostname or IP address.

By default, the switches shall treat all OCSP-related failures as a failure to authenticate the peer device's certificate. Examples of OCSP-related failures include the response signature is invalid, the nonce within the response doesn't match the nonce within the request, or the server is not responding. Additionally, the switch must be configured to have the proper network access to reach the OCSP responder, and configured with an accurate time in order to ensure the OCSP responses are valid.

Should the Security Administrator wish to remove a certificate or CA from the trust store, this can be accomplished with the following commands:

1. To remove an end entity certificate: switch(config)# no crypto pki certificate <name>
2. To remove a struct anchor: switch(config)# no crypto pki ta-profile <name>

Should the Security Administrator wish to clear a private key associated with one or more X.509 certificates stored within the switch, they must zeroize all keys on the switch (including SSH host keys) using the following command: switch(config)# erase all zeroize

## Web Interface

### Cipher Suites

In the evaluated configuration, the following cipher suites are permitted.

- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289

By default, the TOE only supports the preceding cipher suites the secp384r1 curve over TLSv1.2. No other

configuration is necessary.

Aruba CX switches also offer a REST API which uses the same configuration as the web interface. For more information on how to use the REST API, please refer to the 10.11 REST API guide:

[https://www.arubanetworks.com/techdocs/AOS-CX/10.11/PDF/rest\\_v10-0x.pdf](https://www.arubanetworks.com/techdocs/AOS-CX/10.11/PDF/rest_v10-0x.pdf)

## Web Server Certificate

- When configuring the web server certificate, follow the instructions in the Section 'Certificate Installation and Validation' above.
- Once the TA-profile has been configured and the server certificate has been loaded, the administrator should perform the following command to select the appropriate certificate:
  - `switch(config)# crypto pki application https-server certificate <name>`

## Session Resumption

- Session resumption is not enabled by default and no configuration is provided for the administrator to enable it.

## Password Policy and Session Configuration for Web Interface

- The system has one consistent password policy for all supported login mechanisms (web, ssh, console).
- However, the web interface has its own session timeout that's configured separately from the console and SSH server:
  - `switch(config)# https-server session-timeout <value>`

## Secure Remote Logging

All audit events that are generated are logged locally and also sent to all configured syslog servers. The TOE will attempt to transmit the log to the syslog server at the same time it is generated locally. To comply with the evaluated configuration, when logging with a remote syslog server is needed, the connection is secured using TLS. The Syslog client shall compare the Syslog server's FQDN or IPv4 address against the Syslog server's certificate Common Name or Subject Alternative Name. This can be performed through the following commands:

1. Configure logging on the switch to point to the remote syslog server and enable subject name checking for this server:
  - `switch(config)# logging [<IPV4-ADDR> | <IPV6-ADDR> | <HOSTNAME>] tls <PORT-NUM> auth-mode subject-name include-auditable-events severity debug [vrf <VRF-NAME>] Example:`
  - `logging example.com tls auth-mode subject-name include-auditable-events severity debug vrf mgmt`
2. Assign the newly imported certificate to the syslog client:
  - `switch(config-cert-name)# crypto pki application syslog-client certificate <CERT-NAME>`
3. Enable key usage checks for TLS:
  - `switch(config)# tls check-key-usage`

**Note:** While IP address is supported for identity verification, it is recommended that FQDN is used for higher assurance.

To function in the evaluated configuration, the syslog server must be compliant to RFC 5425 (TLS Transport Mapping for Syslog).

Additional information and examples can be found within the following guides:

- [AOS-CX 10.11 Security Guide](#)

- [AOS-CX 10.11 Diagnostics and Supportability Guide](#)

If the connection to the audit server is unintentionally broken, the TLS tunnel must be restarted on the audit server to re-establish the connection.

## Configuring Login Banner

- The evaluated configuration requires the display of an administrator-specified advisory notice before login.
- There are two types of banners:
- MOTD banner – The banner displayed on attempting to connect to a management interface.
- EXEC banner – The banner displayed upon successful authentication.

### Examples

Configuring a banner displayed before the password prompt

```
switch(config)# banner motd ^
```

```
Enter a new banner. Terminate the banner with the delimiter you have chosen.
```

```
>> This is an example of a banner text which a connecting user
```

```
>> will see before they are prompted for their password.
```

```
>>
```

```
>> As you can see it may span multiple lines and the input
```

```
>> will be terminated when the delimiter character is
```

```
>> encountered. ^
```

```
Banner updated successfully!
```

### Configuring a banner displayed after a user has logged on to the switch:

```
switch(config)# banner exec &
```

```
Enter a new banner. Terminate the banner with the delimiter you have chosen.
```

```
>> This is an example of a different banner text. This time
```

```
>> the banner will be displayed after a user has
```

```
>> authenticated.
```

```
>>
```

```
>> & This text will not be included because it comes after the '&'.
```

```
Banner updated successfully!
```

## Finalizing Configuration

### Disabling Services Not Under Evaluation

- The evaluated configuration requires the operator to disable the following services not under evaluation:
- AAA authentication with RADIUS and TACACS+ servers

- AAA accounting with RADIUS and TACACS+ servers
- The operator must issue the following commands to disable the above services:
  - `switch(config)# aaa authentication login default local`

## Booting to Evaluated Configuration

- To save the evaluated configuration, the Administrator must issue the following command:
  - `switch(config)# write mem`
- The above command will commit the evaluated configuration to persistent storage.
- (Please refer to the section “Copying the software and rebooting the switch” to determine which firmware image
  - bank has the desired firmware.)
- Finally, the operator must issue the following command to reboot the switch in the evaluated configuration:
  - `switch(config)# boot system [primary | secondary]`
- The switch will prompt for confirmation:
- Default boot image set to [primary | secondary]
- This will reboot the entire switch and render it unavailable
- Until the process is complete.
  - Continue (y/n)?
- Press [Y] to reboot. When the switch finishes booting, it will be in the evaluated configuration.

## Audit Functionality

### Audit log rotation

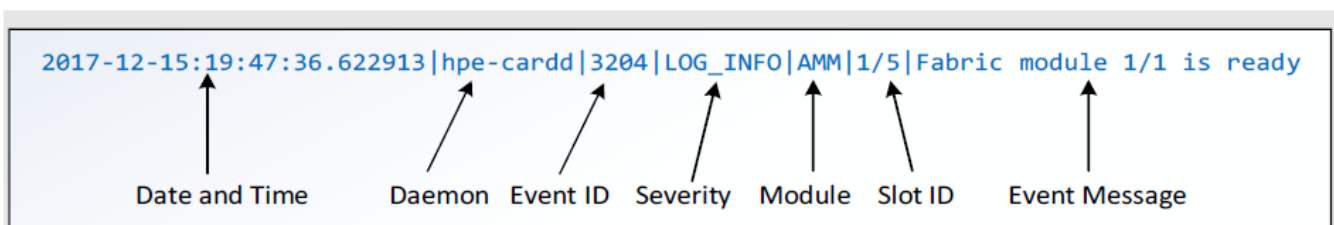
- The logs are rotated based on an administrator-selected log file size threshold (10-200MB) and rotation frequency (hourly, daily, weekly, or monthly) for each log type.
- The TOE stores one working log and up to three old, compressed logs in memory.
- The TOE checks each hour to determine whether or not to rotate its logs based on log size and time elapsed.
- If needed, the TOE will rotate the logs, deleting the oldest compressed log.

### Audit log format

- There are three sources of auditable event logging messages: switch event log, AAA accounting log, and switch authentication log. They have slightly different formats.

### Switch Event Log Format

- For the messages in the switch event log, each log entry is composed of seven fields:



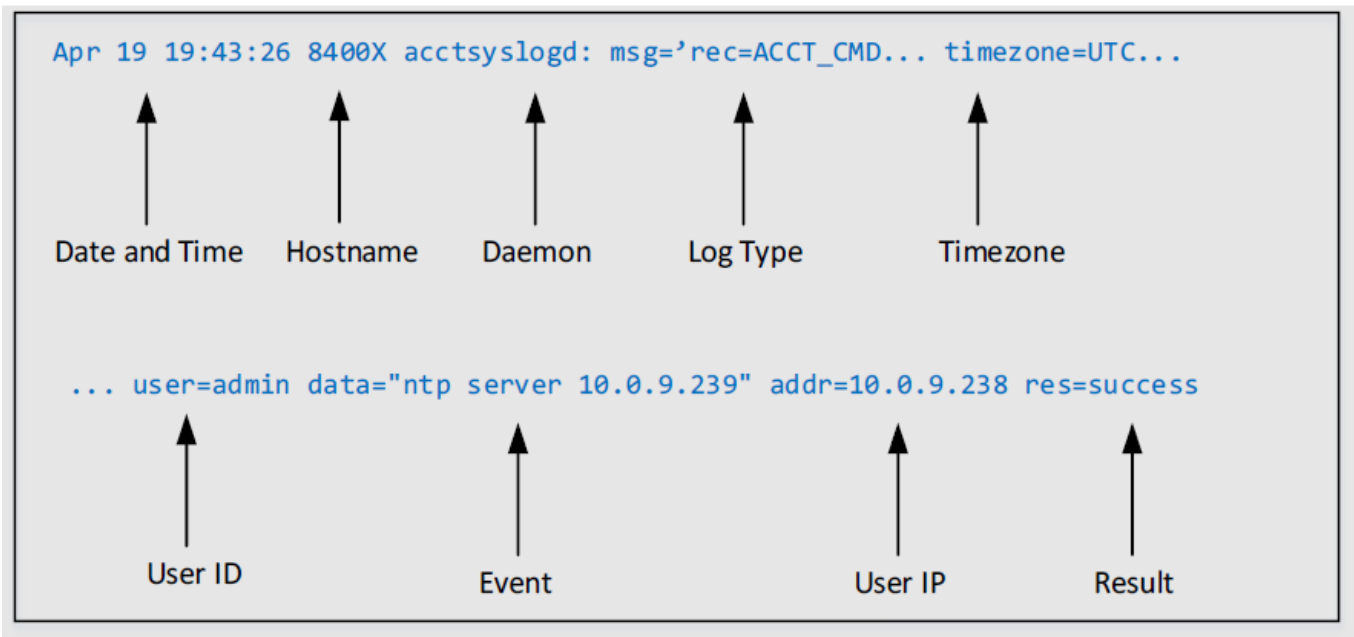


The following table describes each field:  
**TABLE 2 – AUDIT LOG ENTRY ITEMS**

Audit Log Entry Field	Description
Date and Time	The date and time in the format yyyy-mm-dd:hh:mm:ss.xxxxxx when the entry is recorded in the log.
Daemon	The system daemon that generated the log entry.
Event ID	The number assigned to an event.
Severity	One of the following codes (from highest to lowest severity):  <b>LOG_EMERG</b> — the system is unusable.  <b>LOG_ALERT</b> — action must be taken immediately.  <b>LOG_CRIT</b> — critical conditions. <b>LOG_ERR</b> — error conditions. <b>LOG_WARN</b> — warning conditions.  <b>LOG_NOTICE</b> — normal but significant conditions.  <b>LOG_INFO</b> — informational.  <b>LOG_DEBUG</b> — debug level messages.
Module	The management module role that generated the log entry. AMM indicates active management module, and SMM indicates standby management module.
Event Message	A brief description of the operating event

**AAA Accounting Log Format**

For messages from AAA accounting log, each log entry includes the following fields (all on the LOG\_INFO level):



The following table describes each field:  
**TABLE 3 – AUDIT LOG ENTRY ITEMS**

Audit Log Entry Field	Description
Date and Time	The date and time when the entry is recorded in the log.
Daemon	The system daemon that generated the log entry.
Log Type	Represents the type of log entry: ACCT_CMD – Command event. ACCT_EXE C – Login event

Timezone	Timezone of the device.
User ID	The user is tied to this audit log entry.
Event	The command that was issued.
User IP	IP address of the client.
Result	The result of the events: success or failure.

### Switch Authentication Log Format

For messages from the authentication log, each log entry includes the following fields (all on the LOG\_INFO level):

Apr 19 20:56:11 8400X sshd[13276]: Accepted password for admin from 10.0.9.238 port 36490 ...

↑

Date and Time

↑

Daemon

↑

User Identity of the Remote Authentication

Apr 19 20:56:11 8400X systemd-logind[475]: New session c12 of user admin.

↑

Date and Time

↑

Daemon

↑

Session ID and User Identity of the Authenticated User

The following table describes each field:

**TABLE 4 – AUDIT LOG ENTRY ITEMS**

Audit Log Entry Field	Description
Date and Time	The date and time when the entry is recorded in the log.
Daemon	The process which issued this event.
User identity	Includes the IP address and port of the remote host and username of the user logging in.

### List of Auditable Events (As Mandated by the NDcPPe)

**TABLE 5 – SECURITY FUNCTIONAL REQUIREMENTS AND AUDITABLE EVENTS**

Requirement	Auditable Events	<b>Event Message Example</b>  <i>&lt;The audits in the following tables are samples that contain details that will vary based on network addresses, ports, and protocols used by a n installation.&gt;</i>
-------------	------------------	--

FAU_GEN.1	Startup and shutdown of audit functions	Initiating connection to remote syslog server:  2021-04-29T02:03:25.028681-04:00 HPE8320 rsyslogd -- -- nsd_oss! : TLS Connection initiated with remote Syslog server
		Disconnection to remote syslog server:  2021-04-29T02:03:25.066462-04:00 HPE8320 rsyslogd -- -- nsd_oss! : TLS session terminated with remote Syslog server
	Administrative login and logout	Serial (local) login:  2021-02-28T19:20:23.973913-05:00 HPE8320 systemd-logind[279] New session c16 of user admin.
		Serial (local) logout:  2021-05-13T23:17:58.465934-04:00 HPE6300F systemd-logind 607 -- -- Removed session c8..
		Serial (local) login failure:  2021-02-28T19:20:16.505089-05:00 HPE8320 login[8509] FAILED LOGIN (1) on '/dev/ttyS1' FOR 'admin', Authentication failure
		SSH (remote) login:  2021-02-28T19:22:04.387112-05:00 HPE8320 sshd[8744] Accepted password for admin from 192.168.144.254 port 49660 ssh2
		2021-05-07T15:15:06.374118-04:00 HPE8320 sshd 22769 -- -- Accepted publickey for test2 from 192.168.144.253 port 58930 ssh2: RSA.
		SSH (remote) Logout:  sshd[30327]<190>1 2021-04-28T16:34:44.148667-04:00 HPE6300F sshd 30327 -- -- Disconnected from user admin 192.168.144.254 port 51250

		<p>SSH (remote) login failure:</p> <p>2021-02-28T19:22:01.916264-05:00 HPE8320 sshd[8744] Failed password for admin from 192.168.144.254 port 49660 ssh2</p>
		<p>2021-05-07T15:33:12.782396-04:00 HPE8400X sshd 10299 -- Failed</p> <p>publickey for test2 from 192.168.144.253 port 58952 ssh2: RSA</p>
		<p>May 1 19:34:20 8400X sshd[21904]: Connection closed by authenticating user admin 10.0.9.238 port 32930 [preauth]</p>
		<p>REST (WebUI) Login:</p> <p>2023-07-19T15:31:32.985107+00:00 CL-9300 hpe-restd[2487]:</p> <p>Event 4655 LOG_INFO AMM - User sysadmin logged in from 192.168.144.250 through REST session</p>
		<p>REST (WebUI) Logout: 2023-10-20T13:43:55.656627+00:00 CL-9300 hpe-restd[2505]:</p> <p>Event 4657 LOG_INFO AMM - User sysadmin logged out of REST session from 192.168.144.250</p>
		<p>REST (WebUI) login failure: 2023-07-19T15:31:27.198669+00:00 CL-9300 hpe-restd[2487]:</p>

		Event 4656 LOG_ERR AMM - User admin login from
		192.168.144.250 for the REST session has failed
	Change to TSF data related to configuration changes	<p>Configuration change by CLI:</p> <p>2021-05-07T13:53:38.870228-04:00 HPE8320 acctsyslogd -- -- msg=audit op=stop timezone=America/New_York user=admin auth-method=LOCAL data="write memory" addr=192.168.144.254 res=success</p>

Generating cryptographic keys	<p>SSH host-key generation:</p> <p>2024-02-22T00:45:04.027827+00:00 myswitch ssh-utild[3055]:</p> <p>Event 5201 LOG_INFO AMM 1/1 SSH host-key rsa_4096 is installed.</p> <p>24-02-22T01:04:22.649665+00:00 myswitch hpe-credmgr[2201]: Event 6506 LOG_INFO AMM 1/1 SSH authorized keys were added for user admin</p>
	<p>MACsec:</p> <p>2024-02-23T04:35:58.798720+00:00 8360 acctsyslogd[355]:</p> <p>AUDIT CLI "pre-shared-key can 123456 cak plaintext 123456" executed by user 'admin' from address '0.0.0.0' through CONSOLE session which resulted in success at timezone UTC.</p>
Import of cryptographic keys	<p>&lt;190&gt;1 2024-02-23T23:55:04.715015+00:00 6100 acctsyslogd 2693</p> <p>–</p> <p>– AUDIT CLI "crypto pki certificate myleafcert" executed by user 'admin' from address '0.0.0.0' through CONSOLE session which resulted in success at timezone UTC.</p> <p>&lt;190&gt;1 2024-02-23T23:55:36.471779+00:00 6100 acctsyslogd 2693</p> <p>–</p> <p>– AUDIT CLI "import terminal self-signed" executed by user 'admin' from address '0.0.0.0' through CONSOLE session which resulted in success at timezone UTC.</p>
Changing cryptographic keys	<p>&lt;190&gt;1 2024-02-24T00:33:06.251505+00:00 6100 acctsyslogd 2693</p> <p>–</p> <p>– AUDIT CLI "crypto pki application https-server certificate myleafcert" executed by user 'admin' from address '0.0.0.0' through CONSOLE session which resulted in success at timezone UTC.</p>
Deleting cryptographic keys	<p>2024-02-22T00:53:30.970286+00:00 myswitch certmgr[605]:</p> <p>Event 7704 LOG_INFO AMM 1/1 Leaf certificate mycert deleted</p>

		<p>MACsec:</p> <p>2024-02-23T04:36:07.598948+00:00 8360 acctsyslogd[355]:</p> <p>AUDIT CLI “no pre-shared-key can 123456 cak plaintext 123456” executed by user ‘admin’ from address ‘0.0.0.0’ through CONSOLE session which resulted in success at timezone UTC.</p>
	Resetting passwords (name of related user account shall be logged).	<p>2024-02-22T00:47:07.468112+00:00 my switch -vtysh[2621]:</p> <p>Event 4703 LOG_INFO AMM 1/1 User admin successfully changed password</p>
	Disabling services not under	<p>2024-02-22T00:48:33.907613+00:00 my switch ntp-mgrd[2656]:</p> <p>Event 1107 LOG_INFO   NTP enable state change: NTP is enabled – &gt; NTP is disabled</p>

	evaluation	
FAU_GEN.2	None.	
FAU_STG_EXT.1	None.	
FCS_CKM.1	None.	
FCS_CKM.2	None.	
FCS_CKM.4	None.	
FCS_COP.1/ DataEncryption	None.	
FCS_COP.1/SigGen	None.	
FCS_COP.1/Hash	None.	
FCS_COP.1/ KeyedHash	None.	
FCS_RBG_EXT.1	None.	

FCS_SSHS_EXT.1	Failure to establish an SSH session	<p>sshd[5005]&lt;190&gt;1 2020-12-07T11:45:33.677860-05:00 HPE8320 sshd</p> <p>5005 -- Unable to negotiate with 192.168.144.254 port 39364: no matching cipher found. Their offer: <a href="#">aes128-gcm@openssh.com</a> [preauth]</p>
		<p>sshd[5663]&lt;190&gt;1 2020-12-07T11:55:17.262452-05:00 HPE8320 sshd</p> <p>5663 -- Unable to negotiate with 192.168.144.254 port 40510: no matching host key type found. Their offer: ssh-rsa [preauth]</p>
		<p>sshd[6271]&lt;190&gt;1 2020-12-07T12:03:43.811286-05:00 HPE8320 sshd</p> <p>6271 -- Unable to negotiate with 192.168.144.254 port 41514: no matching MAC found. Their offer: hmac-sha1-96 [preauth]</p>
		<p>sshd[6479]&lt;190&gt;1 2020-12-07T12:05:56.028125-05:00 HPE8320 sshd</p> <p>6479 -- Unable to negotiate with 192.168.144.254 port 42088: no matching key exchange method found. Their offer: ecdh-sha2-nistp521,ext-info-c [preauth]</p>
		<p>2023-06-01T12:59:50.875471+00:00 my switch sshd 6701 -- Bad packet length 262156.</p>
FCS_TLSC_EXT.1, FCS_TLSS_EXT.1, FCS_HTTPS_EXT.1, FIA_X509_EXT.1/Rev	Failure to establish a TLS Session	<p>SAN/CN Mismatch IP and Hostname:</p> <p>2021-03-21T22:30:13.565-04:00 myswitch rsyslogd[4043]: debug LOG_ERR    Certificate SAN/CN doesn't match the peer name tl34-16x.example.com.</p> <p>2023-09-20T18:02:26.407908+00:00 CL-9300 rsyslogd 43321 -- Event 7709 LOG_WARN AMM 1/1 Certificate bar*.example.com rejected due to verification failure (20)</p>
		<p>Cert Validation error:</p> <p>2021-03-21T22:44:05.883550-04:00 HPE8400X rsyslogd: nsd_ossli: not permitted talk to peer: certificate validation failed. Status Code : 20 [v8.36.0 try <a href="http://www.rsyslog.com/e/2090">http://www.rsyslog.com/e/2090</a> ]</p>
		<p>Missing Server Purpose:</p>

		<p>2023-08-24T22:50:30.475389+00:00 myswitch rsyslogd -- nsd_ossli: not permitted to talk to peer: certificate validation failed. Status Code : 74 [v8.1908.0 try <a href="https://www.rsyslog.com/e/2090">https://www.rsyslog.com/e/2090</a> ] Expire</p>
--	--	--

d Cert:

2021-03-22T00:27:34.447-04:00 my switch rsyslogd[4369]: debug|LOG\_ERR||The certificate is expired

Revoked Cert:

2023-09-05T17:18:13.808035+00:00 myswitch rsyslogd ---  
nsd\_oss! not permitted to talk to peer: certificate validation failed. Status Code: 46 [v8.1908.0 try <https://www.rsyslog.com/e/2090> ]

Unreachable OCSP:

2023-09-18T20:12:08.552881+00:00 myswitch rsyslogd 137812 ---

Event|7709|LOG\_WARN|AMM|1/1|Certificate tl24- 16x.example.com rejected due to verification failure (37) OCSP failed verification:

2023-08-28T20:37:05.423428+00:00 myswitch rsyslogd ---  
nsd\_oss! not permitted to talk to peer: certificate validation failed. Status Code: 42 [v8.1908.0 try <https://www.rsyslog.com/e/2090> ]

Bad signature:

2023-08-26T19:49:49.159838+00:00 myswitch rsyslogd ---  
nsd\_oss! not permitted to talk to peer: certificate validation failed. Status Code: 10 [v8.1908.0 try <https://www.rsyslog.com/e/2090> ]

Missing Basic constraints:

2023-08-27T19:53:52.001230+00:00 myswitch rsyslogd ---  
nsd\_oss! not permitted to talk to peer: certificate validation failed. Status Code: 12 [v8.1908.0 try <https://www.rsyslog.com/e/2090> ]

Explicit elliptic curve:

2023-09-06T12:21:37.488866+00:00 myswitch rsyslogd ---  
nsd\_oss! not permitted to talk to peer: certificate validation failed. Status Code: 78 [v8.1908.0 try <https://www.rsyslog.com/e/2090> ]

Broken chain:

2023-07-23T20:26:19.888649+00:00 myswitch rsyslogd ---  
nsd\_oss! not permitted to talk to peer: certificate validation failed. Status Code: 10 [v8.1908.0 try <https://www.rsyslog.com/e/2090> ]

Wrong extended key usage:

2023-07-23T22:49:29.475389+00:00 myswitch rsyslogd ---  
nsd\_oss! not permitted to talk to peer: certificate validation failed. Status Code: 74 [v8.1908.0 try <https://www.rsyslog.com/e/2090> ]



		<p>No Matching Cipher:</p> <p>2023-08-22T23:46:12.206582+00:00 my switch rsyslogd --- nsd_ossl:OpenSSL Error Stack: error:140920F8:SSL routines:ssl3_get_server_hello:unknown cipher returned [v8.1908.0]</p> <p>Bad record MAC:</p> <p>2023-08-22T23:53:54.406696+00:00 myswitch rsyslogd --- nsd_ossl:OpenSSL Error Stack: error:1408F119:SSL routines:SSL3_GET_RECORD:decryption failed or bad record mac [v8.1908.0]</p>
--	--	--

		<p>Wrong TLS Version:</p> <p>2023-08-22T23:49:28.253698+00:00 my switch rsyslogd --- nsd_ossl:OpenSSL Error Stack: error:1409210A:SSL routines:ssl3_get_server_hello:wrong SSL version [v8.1908.0]</p> <p>Handshake Failure:</p> <p>2023-08-23T17:38:18.289958+00:00 myswitch rsyslogd --- nsd_ossl:OpenSSL Error Stack: error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure [v8.1908.0]</p> <p>Wrong certificate type:</p> <p>2023-08-22T23:45:16.866679+00:00 my switch rsyslogd --- nsd_ossl:OpenSSL Error Stack: error:1409017F:SSL routines:ssl3_get_server_certificate:wrong certificate type [v8.1908.0]</p>
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	<p>Failed login attempt from SSH or Local console as described by FAU_GEN.1 audit contains the Origin of the Attempt.</p> <p>2023-05-15T19:41:20.230216+00:00 DL-10000 log-proxyd 942 --- Event[5210 LOG_ERR AMM 1/1 User test login from 192.168.144.254 for SSH session failed during password-based authentication.</p> <p>AND</p> <p>Login Attempt Limit is exceeded:</p> <p>2021-05-07T16:19:39.868469-04:00 HPE8320 sshd 25938 --- pam_tally2(sshd: auth): user test (1004) tally 6, deny 2</p>

FIA_PMG_EXT.1	None.	
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	See the row for FAU_GEN.1 above.
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	See the row for FAU_GEN.1 above.
FIA_UAU.7	None.	
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update.	<p>Upon user types in CLI "copy sftp:// ... ..":</p> <p>2020-12-11T11:28:17.539060-05:00 HPE8320 acctsyslogd -- --</p> <p>msg=audit op=stop timezone=America/New_York user=admin auth-method=LOCAL data="copy tftp://192.168.144.253/TL_10_06_0010T.swi primary vrf mgmt" addr=0.0.0.0 res=success</p> <p>2020-12-11T11:28:17.536493-05:00 HPE8320 -vtysh 22197 --</p> <p>Event 4401 LOG_INFO AMM 1/1 User admin: primary image updated via TFTP from 192.168.144.253. Firmware version, Before Update: TL.10.01.0001 After Update: TL.10.06.0010T</p>

		<p>2021-01-29T10:40:59.371151-05:00 HPE8320 -vtysh 14571 --</p> <p>Event 4403 LOG_ERR AMM 1/1 User admin: secondary image update failed via TFTP from 192.168.144.253</p>
FMT_MTD.1/ CoreData	None.	
FMT_SMF.1	All management activities of TSF data.	Ability to administer the TOE locally and remotely: See the row for FAU_GEN.1 above.
		Ability to configure the access banner:
		<p>2023-10-25T14:48:14.960308+00:00 DL-10000 acctsyslogd -- --</p> <p>msg=audit op=stop timezone=UTC user=gssadmin auth-method=LOCAL data="banner exec /" addr=192.168.144.254 res=success</p>

		Ability to update the TOE, and to verify the updates using [digital signature] capability before installing those updates: See the row for FMT_MOF.1/ManualUpdate above.
		Ability to configure the session inactivity time before session termination or locking:
		2023-06-01T17:50:05.676402+00:00 my switch acctsyslogd --- msg=audit op=stop timezone=GMT user=gssadmin auth-method=LOCAL data="session-timeout 1" addr=192.168.144.254 res=success
		Ability to configure the authentication failure parameters for FIA_AFL.1:
		2023-06-01T12:39:24.846116+00:00 my switch acctsyslogd --- msg=audit op=stop timezone=UTC user=gssadmin auth-method=LOCAL data="aaa authentication limit-login-attempts 3 lockout-time 120" addr=192.168.144.254 res=success
		Ability to modify the behavior of the transmission of audit data to an external IT entity:
		2023-10-24T12:33:58.362730+00:00 FL-6300M acctsyslogd --- msg=audit op=stop timezone=UTC user=gssadmin auth-method=LOCAL data="logging tl24-16x.example.com tls auth-mode subject-name include-auditable-events severity debug vrf mgmt" addr=192.168.144.254 res=success
		Ability to configure the cryptographic functionality:
		SSH public key authentication:
		Enable:  2024-01-08T13:37:16.146086+00:00 LL-8360v2 acctsyslogd --- msg=audit op=stop timezone=UTC user=gssadmin auth-

		method=LOCAL data="ssh public-key-authentication"
		addr=192.168.144.254 res=success
		Disable:
		2024-01-08T13:37:10.018864+00:00 LL-8360v2 acctsyslogd ---
		msg=audit op=stop timezone=UTC user=gssadmin auth-

	method=LOCAL data="no ssh public-key-authentication"
	addr=192.168.144.254 res=success
	For others, see the relevant FAU_GEN.1 entries.
	Ability to set the time which is used for time-stamps:
	See FPT_STM_EXT.1.
	Ability to manage the TOE's trust store and designate X509.v3
	certificates as trust anchors:
	2024-02-22T02:13:17.419264+00:00 6100 certmgr[608]:
	Event 7701 LOG_INFO AMM 1/1 TA Profile test-ca created
	Ability to import X509v3 certificates to the TOE's trust store:
	2023-08-29T17:09:21.956815+00:00 FL-6300M acctsyslogd - - -
	msg=audit op=stop timezone=UTC user=gssadmin auth-
	method=LOCAL data="crypto pki ta-profile root ca-rsa"
	addr=192.168.144.254 res=success
	2023-10-25T13:02:07.334259+00:00 FL-6300M acctsyslogd - - -
	msg=audit op=stop timezone=UTC user=gssadmin auth-
	method=LOCAL data="ta-certificate import terminal"
	addr=192.168.144.254 res=success
	Ability to manage the trusted public keys database:
	2024-02-22T02:13:17.419264+00:00 6100 certmgr[608]:
	Event 7701 LOG_INFO AMM 1/1 TA Profile test-ca created
	2024-02-22T03:02:23.972375+00:00 6100 certmgr[608]:
	Event 7702 LOG_INFO AMM 1/1 TA Profile test-ca deleted

FMT_SMF.1/MACSEC.1	TSF management functions related to MACSEC functionality	<b>Manage a PSK-based CAK and install it in the device:</b>  2023-11-06T14:11:37.970068+00:00 FL-6300M acctsyslogd --- msg=audit op=stop timezone=UTC user=gssadmin auth- method=LOCAL data="pre-shared-key ckn1234567890123456789012345678901234567890123456789064 cak plaintext 410a" addr=192.168.144.254 res=success
		<b>Manage the Key Server to create, delete, and activate MKA participants:</b>
		Create/Activate:

		<p>2024-02-12T03:30:23.414+00:00 acctsyslogd[374]: AUDIT CLI "apply aka policy cx" executed by user 'admin' from address '0.0.0.0' through CLI session which resulted in success at timezone UTC.</p> <p>Delete:</p> <p>2024-02-12T03:41:02.864+00:00 acctsyslogd[374]: AUDIT CLI "no apply mka policy cx" executed by user 'admin' from address '0.0.0.0' through CLI session which resulted in success at timezone UTC.</p> <p><b>Specify a lifetime of a CAK:</b></p> <p>2024-01-04T19:30:23.904617+00:00 LL-8360v2 acctsyslogd -- --</p> <p>msg=audit op=stop timezone=UTC user=gssadmin auth- method=LO CAL data="send-lifetime start-time 10:10:10 1/4/2023 end-time 10:10:10 2/4/2023" addr=0.0.0.0 res=success</p> <p><b>Enable, disable, or delete a PSK-based CAK:</b></p> <p>Enable:</p> <p>2023-11-06T14:27:23.762359+00:00 LL-8360v2 acctsyslogd -- --</p> <p>msg=audit op=stop timezone=UTC user=gssadmin auth- method=LO CAL data="pre-shared-key ckn 1234567890123456789012345678901212345678901234567890123456789064 cak plaintext 410a" addr=192.168.144.254 res=success</p> <p>Disable / delete:</p> <p>2024-01-08T14:52:57.757947+00:00 LL-8360v2 acctsyslogd -- --</p> <p>msg=audit op=stop timezone=UTC user=gssadmin auth- method=LO CAL data="no pre-shared-key can 1000 cak plaintext 12345678901234567890123456789012" addr=192.168.144.254</p> <p>res=success</p>
FMT_SMR.2	None.	
FPT_SKP_EXT.1	None.	
FPT_APW_EXT.1	None.	
FPT_TST_EXT.1	None.	

FPT_TUD_EXT.1	Initiation of update; the result of the update attempt (success or failure)	See the row for FMT_MOF.1/ManualUpdate above.
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process.  (Note that no continuous changes to time need to	Upon user types in “clock date 2021-04-26 ”:  2021-04-26T22:53:33.008601-04:00 HPE8320 -stylish 2889 – –  Event 6202 LOG_INFO AMM 1/1 System date/time changed from 2021-03-31 15:01:41 to 2021-04-26 22:53:33

	be logged. See also the application note on FPT_STM_EXT.1)	
FTA_SSL_EXT.1 (if “lock the session” is selected)	Any attempts at unlocking an interactive session.	NA
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.	Upon local (serial) session timeout:  2021-05-13T23:17:58.465934-04:00 HPE6300F systemd-logind 607 – –  Removed session c8.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	Upon remote (SSH) session timeout:  2021-05-13T23:25:21.454172-04:00 HPE6300F sshd 7165 – –  Disconnected from user admin 192.168.144.254 port 59114

FTA_SSL.4	The termination of an interactive session.	<p>Upon the user types “exit” from a remote session:</p> <p>2021-04-28T16:34:44.148667-04:00 HPE6300F sshd 30327 – –</p> <p>Disconnected from user admin 192.168.144.254 port 51250.</p> <p>Upon the user types “exit” from a local session:</p> <p>2023-06-05T13:46:30.240991+00:00 myswitch log-proxyd 1844 – – Event 13003 LOG_INFO AMM 1/1 User admin logged out of CONSOLE session from 0.0.0.0.</p> <p>Upon the user types “exit” from an HTTPS session:</p> <p>2023-07-19T17:58:17.248276+00:00 my switch hpe-restd[2487]:</p> <p>Event 4657 LOG_INFO AMM - User admin logged out of REST session from 192.168.144.250</p>
FTA_TAB.1	None.	
FTP_ITC.1	<p>Initiation of the trusted channel.</p> <p>Termination of the trusted channel.</p>	<p>2023-10-24T12:33:58.362730+00:00 FL-6300M acctsyslogd – – –</p> <p>msg=audit op=stop timezone=UTC user=gssadmin auth-method=LOCAL data=”logging tl24-16x.example.com tls auth-mode subject-name include-auditable-events severity debug vrf mgmt” addr=192.168.144.254 res=success</p> <p>2021-03-21T22:27:19.698671-04:00 HPE8400X rsyslogd – – –</p> <p>nsd_oss! TLS Connection initiated with a remote syslog server. [v8.36.0]</p> <p>2021-03-21T22:27:19.755427-04:00 HPE8400X rsyslogd 32000 – –</p> <p>Event 7708 LOG_INFO UMM - Certificate tl34-16x.example.com verified and accepted</p> <p>2023-08-23T17:51:54.082951+00:00 myswitch rsyslogd – – – nsd_oss! TLS session terminated with a remote syslog server. [v8.1908.0]</p>



FTP_TRP.1/Admin	Initiation of the trusted path.  Termination of the trusted path. Failure of the trusted path functions.	2023-10-16T13:35:44.448500+00:00 FL-6300M hpe-restd[1282]:  Event 4660 LOG_INFO AMM - REST server is enabled on VRF mgmt.  See the row for FAU_GEN.1 on SSH (remote) and HTTPS login and logout above.
-----------------	--	--

## Self Tests

The switch will perform a series of self-tests upon booting from a power cycle, or from the CLI boot command. Self-tests are designed to verify the integrity of cryptographic functions, and as such are run before any cryptographic functionality is invoked. Should any tests fail, the switch will enter an error state.

The switch will perform the following tests:

The following KAT self-tests are performed at boot:

- HMAC-SHA1 of the cryptographic library
- AES encrypt/decrypt
- AES GCM
- AES-CCM
- XTS-AES
- AES CMAC
- Triple-DES CMAC
- ECDH
- HMAC-SHA1
- HMAC-SHA224
- HMAC-SHA256
- HMAC-SHA384
- HMAC-SHA512
- RSA
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512
- SP 800-90 DRBG (Hash\_DRBG, HMAC\_DRBG, CTR\_DRBG)
- Triple-DES encrypt/decrypt
- ECC CDH

The following pair-wise consistency self-tests are performed at boot:

- DSA
- RSA

- ECDSA

In the event of a test failure, the switch will crash with a message similar to the following:  
FIPS POST: Cryptographic self-test started...FAILED

- The switch validates firmware at every boot. Please refer to the Firmware Validation section above for more details.
- If the switch firmware validation fails at boot, the switch will fail to boot with one of the following error messages and drop the user into the ServiceOS login screen:
  - Error: Signature verification failed
  - Error: Signature not found
  - Error: Invalid signature
- If a selftest failure occurs, please reboot the device or load new firmware.

## **Key Destruction**

- Keys are not saved to persistent storage until the “write memory” command has been issued or the running configuration is saved to the startup configuration:
  - switch# write memory
  - switch# copy running-config startup-config
- Key destruction is delayed at the physical layer until the “write memory” command has been issued.

## **Appendix A: MACsec Configuration**

### **Auditable Events**

Requirement	Auditable Events	Event Message Example
FCS_MACSEC_EXT.1	Session establishment with Secure Channel Identifier (SCI)	2023-10-12T18:32:55.006464+00:00  myswitch macsecd 4678 -- Event 11201 LOG_INFO CDTR 1 MACsec session established on Rx Secure Channel 00155d00f90d0001 on interface 1/1/2.
FCS_MACSEC_EXT.3	Creation of SAK with creation time	2023-07-19T11:37:53.722978+00:00  my switch missed 4775 -- Event 11203 LOG_INFO CDTR 1 Secure Association key updated for Connectivity Association 1000 on interface 1/1/1 -- Latest AN/KN 2/3, Old AN/KN 0/0
		* Note: Old AN/KN 0/0 indicates a create event
	Update of SAK with update time	2023-11-09T17:48:49.822830+00:00  myswitch macsecd 3469 -- Event 11203 LOG_INFO AMM 1/1 Secure Association key updated for Connectivity Association 1000 on interface 1/1/2 -- Latest AN/KN 2/3, Old AN/KN 1/2.
		* Note: Old AN/KN of non-zero values indicates an update
FCS_MACSEC_EXT.4	Creation of CA with Connectivity Association Key Names (CKNs)	2023-10-12T18:32:55.007009+00:00  myswitch macsecd 4678 -- Event 11202 LOG_INFO CDTR 1 MKA session secured for Connectivity Association 1000 on interface 1/1/2.
FPT_RPL.1	Detected replay attempt	2023-10-12T18:32:57.191638+00:00  myswitch macsecd 4678 -- Event 11204 LOG_INFO CDTR 1 Possible replay attempt detected on the Secure Channel 00155d00f90c0001.

## MACsec Policy Configuration

- For full instructions on the configuration of MACsec, please see the section 'MACsec' in the AOS-CX 10.11 Security Guide. The instructions below are specific to the configuration for Common Criteria and the evaluated configuration.

## MACsec Configuration (using pre-shared keys)

- Create the MACsec Policy:

When configuring the MACsec policy, GCM cipher suites are supported, with both 128-bit and 256-bit AES keys. Extended Packet Numbering (XPN) cipher suites are supported in furtherance of FPT\_RPL\_EXT.1 and may also be used.

```
switch(config)# macsec policy <Policy_Name>

switch(config-macsec-policy)# cipher-suite gcm-aes-256 gcm-aes-xpn-256

switch(config-macsec-policy)# replay-protection window-size 100

switch(config-macsec-policy)# exit
```

2. Create and configure MKA Policy:

```
switch(config)# mka policy <Policy_Name>

switch(config-mka-policy)# pre-shared-key ckn <key> cak plaintext <key>

switch(config-mka-policy)# key-server-priority 5

switch(config-mka-policy)# exit
```

3. Apply the MACsec and MKA Policy to the port range:

```
switch(config)# interface 1/1/1-1/1/4

switch(config-if-<1/1/1-1/1/4>)# apply macsec policy <Policy_Name>

switch(config-if-<1/1/1-1/1/4>)# apply mka policy <Policy_Name>

switch(config-if-<1/1/1-1/1/4>)# exit
```

The pre-shared key is comprised of the administrator-supplied CKN and CAK. Switches do not auto-generate PSKs. Both the CKN and CAK are hexadecimal character inputs.

- pre-shared-key keychain <NAME>
- pre-shared-key can <CA-KEY-NAME> cak {plaintext [<PLAINTEXT-CAK>] | ciphertext <CIPHERTEXT-CAK>}

The CKN supports a range of 1 to 64 hexadecimal characters. Longer CKN values are stronger.

### MACsec Configuration (using 802.1X EAP TLS)

- 802.2X EAP TLS is not part of the evaluated configuration and should not be used.

### Configuration of Confidentiality

- To configure and apply the confidentiality offset to a macsec-policy, the security administrator should apply the following command:
  - switch(config-macsec-policy)# confidentiality [offset {0|30|50}]
- To remove the confidentiality setting, the administrator can enter 'no confidentiality'. In the evaluated configuration, this should only be done when changing a configuration.
- Refer "confidentiality" sub-section under the MACsec commands section in the Security Guide for additional information.

## Configuration of SCI tag

- Within the MACsec policy context, enables the inclusion of the Secure Channel Identifier (SCI) tag in the Security TAG (SecTAG) field of the MACsec header. This is the default. Inclusion of the SCI tag is not required on point-to-point links if the transmitting link has only one MACsec peer.
- Enabling the SCI tag:
  - `switch(config-macsec-policy)# include-sci-tag`
- Disabling the SCI tag:
  - `switch(config-macsec-policy)# no include-sci-tag`
- Refer “include-sci-tag” sub-section under the MACsec commands section in the Security Guide for additional information.

## Configuration for Replay Protection

- Within the MACsec policy context, enables replay protection with the default or specified window size. With replay protection enabled, packets are expected to arrive within the replay protection window number of packets. For
  - example, with a window size of 10, any packet arriving out-of-sequence by more than 10 packets will be discarded. A window size of 0 (the default) enforces strict order of packet reception, discarding all packets not received in
  - perfect sequence. The no form of this command disables replay protections and resets the window size to its 0 default.
  - `switch(config-macsec-policy)# replay-protection`
  - `switch(config-macsec-policy)# replay-protection window-size 100`
- Refer “replay-protection” sub-section under the MACsec commands section in the Security Guide for additional information.

## Configuration of CAK Lifetime

- When configuring the lifetime of the CAK, the administrator should apply a specified lifetime to the applied key chain. This can be done through usage of the ‘send-lifetime’ command.
  - `switch# configure terminal`
  - `switch(config)# keychain ospf_keys`
  - `switch(config-keychain)# key 1`
- With start and end date:
  - `switch(config-keychain-key)# send-lifetime start-time 10:10:10 10/25/2020 end-time 10:10:10 11/25/2020`
- With start date and duration:
  - `switch(config-keychain-key)# send-lifetime start-time 10:10:10 10/25/2020 duration 1000`
- Ability to specify infinite duration with a specified start date:
  - `switch(config-keychain-key)# send-lifetime start-time 10:10:10 10/25/2020 duration infinite`
- Changing to include the end time:
  - `switch(config-keychain-key)# send-lifetime end-time 10:10:10 11/25/2020`
- Changing to specify duration:
  - `switch(config-keychain-key)# send-lifetime duration 1000`

- Changing to have an infinite lifetime:
  - `switch(config-keychain-key)# send-lifetime duration infinite`
- Refer to the 'keychain' chapter in the CLI Guide and the sub-section pre-shared key under MKA policy in the Security Guide for description and examples on configuring a CAK with lifetime via keychains.
- The lifetime can be viewed by using the 'show running-config keychain' command.

## Key Server Priority

- In the config-mka-policy policy context, configure the MKA key server priority. The highest priority is 0 and indicates that this switch strongly wants to be the MKA key server. The lowest priority is 255 which indicates that the switch does not want to be the MKA key server, allowing the switch at the other end of the link to be the key server. Set this priority on the switches at either end of the link to achieve the desired effect.
- If the key server priority is 0 on both switches then the switch with the lowest system MACsec address is elected as key server. No other configuration is necessary by the administrator.
  - `switch(config-mka-policy)# key-server-priority 5`

## MACsec Selftest

- To ensure that self-tests for MACsec, as well as FIPS module and entropy source health tests, result in secure failure, the selftest mode must be set to fail-secure
  - `Switch(config)# macsec selftest`
  - `Switch(config)# selftest fail-secure`
- If a self-test is failed, an EMERGENCY log will be issued, and the switch will immediately reboot. The reboot loop will continue as long as the self-test continues to fail.

## Appendix B: Documentation References


### Aruba Switch Series Documentation References

- Access the HPE Networking products page to obtain the up-to-date documents of Aruba Switches:
- <http://h17007.www1.hpe.com/us/en/networking/library/#.WqnKvTaWzSd>
- Search on the products and select from the models listed. Links will be provided with information about the product, such as a datasheet, installation manual, configuration guide, command reference, and other reference documents.
- More information is available on the full line of products for Aruba from the following sources:
  - HPE website ([www.hpe.com](http://www.hpe.com))
  - Aruba website ([www.arubanetworks.com](http://www.arubanetworks.com))

## Technical support

- For technical or sales-related questions please refer to the contacts list on the HPE website: <http://www.hpe.com>

## Documents / Resources

 Common Criteria Administrator Guidance HPE Aruba Networks HPE Aruba Networks HPE Aruba Networks HPE Aruba Networks	<a href="#">HPE 8360v2 Switch Series</a> [pdf] User Guide 8360v2 Switch Series, 8360v2, Switch Series, Series
---	--

References

- [User Manual](#)

Manuals+, Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.