Common Criteria

Administrator Guidance

Target of Evaluation: Aruba 4100, 6000, 8000, 9000, and 10000 Switch Series

Version 2.5

May 6, 2024

Table of Contents

TABLE OF TABLES and FIGURES

1 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 have knowledge of 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 10.13, 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 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.

2 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

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 or HTTPS browser 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.

Connecting to the Rest API Interface through 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. Login to the TOE through the REST API interface by submitting a POST operation to

    https://<IP address>/rest/v10.04/login

Username and Password must also be provided with this POST action. Preferably these values are provided as protected data in the TLS exchange (i.e., using the –F argument of CURL). They can also be provided as part of the URL query string. However, submitting passwords as a query string has the potential to exposes the passwords. Thus, submitting these variables and values as protected data in the TLS exchange is recommended.

A RestAPI session can be terminated using the following RestAPI POST operation:

https://<IP address>/rest/v10.04/logout

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 addressing 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 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
    ```

    In the event that 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 serviceos
   ```

   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, login as 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. 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 username set to **admin** and no password. You set the administrator account password as part of the initial configuration procedure for the switch.

Once in secure mode, the switch does not offer any management services or access to its management functions, except for displaying a warning banner, without requiring a user to be identified and authenticated.

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 lower case 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 combination of the 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 for a local or remote command line interface (CLI) session. The default setting is 30 minutes.

```
switch(config)# session-timeout <value in minutes>
```

Issue the following command to terminate the local or remote CLI session:

```
switch# exit
```

NOTE: The actual termination may take 5-30 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.

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 login to the switch using the management interfaces SSH or Console. 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 Administrators and Operators username and passwords to control access privileges from the console and other management interfaces. To log out from 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 transferred, whichever occurs first. This is performed to address a common security concern that encryption/decryption keys not be used for long periods of time. 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# show 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 which 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 desired preference of algorithms.

Certificate Installation and Validation

X.509 digital certificates are used by the Secure Remote Logging feature and allows 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 that 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 extendedKeyUsage extension when the peer device is acting as a server.

5. Verifies the presence of the Client Authentication purpose bit is set within the extendedKeyUsage extension when the peer device is acting as a client.
6. Verifies the presence of the OCSP Signing purpose bit is set within the extendedKeyUsage 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 host name 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 OSCP 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 for use when the Aruba CX switch is a TLS server.

- 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 Aruba CX switch only supports the preceding cipher suites with a key exchange using 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 10.13 REST API guide: https://www.arubanetworks.com/techdocs/AOS-CX/10.13/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. The following command specifies the inactivity timeout value for the Web interface and RestAPI interface:

```
switch(config)# https-server session-timeout <value>
```

NOTE: The actual termination may take 30 seconds longer than the configured value, administrators should set this value accordingly.

To terminate a Web session, the user can perform ‘logout’ operation that can be found as a pulldown menu under the “user management” icon at the top of the Web page

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 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). The following cipher suites are permitted for use when the Aruba CX switch is a TLS client.

- 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 Aruba CX switch only supports the preceding cipher suites, no configuration is necessary or possible.

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

AOS-CX 10.13 Security Guide
AOS-CX 10.13 Diagnostics and Supportability Guide

In the event that 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 prior to 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

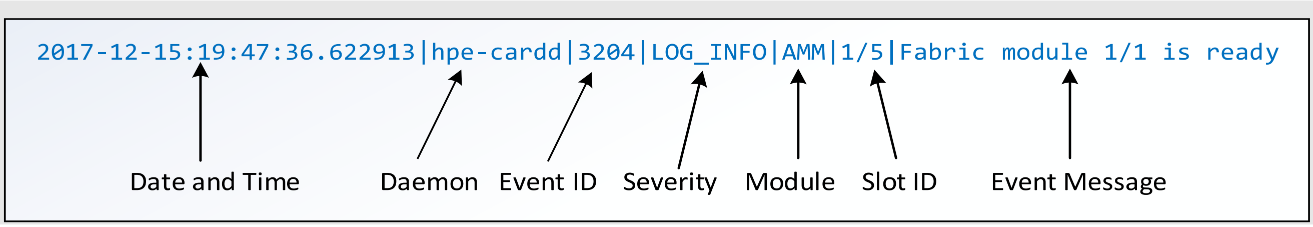
The logs are rotated based on an administrator selected log file size threshold (10-200MB) and rotation frequency (hourly, daily, weekly, or monthly) for each log type. The TOE stores a working log and old, compressed logs in memory. The TOE checks each hour to determine whether or not to rotate its logs based upon 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:



```
2017-12-15:19:47:36.622913|hpe-cardd|3204|LOG_INFO|AMM|1/5|Fabric module 1/1 is ready
```

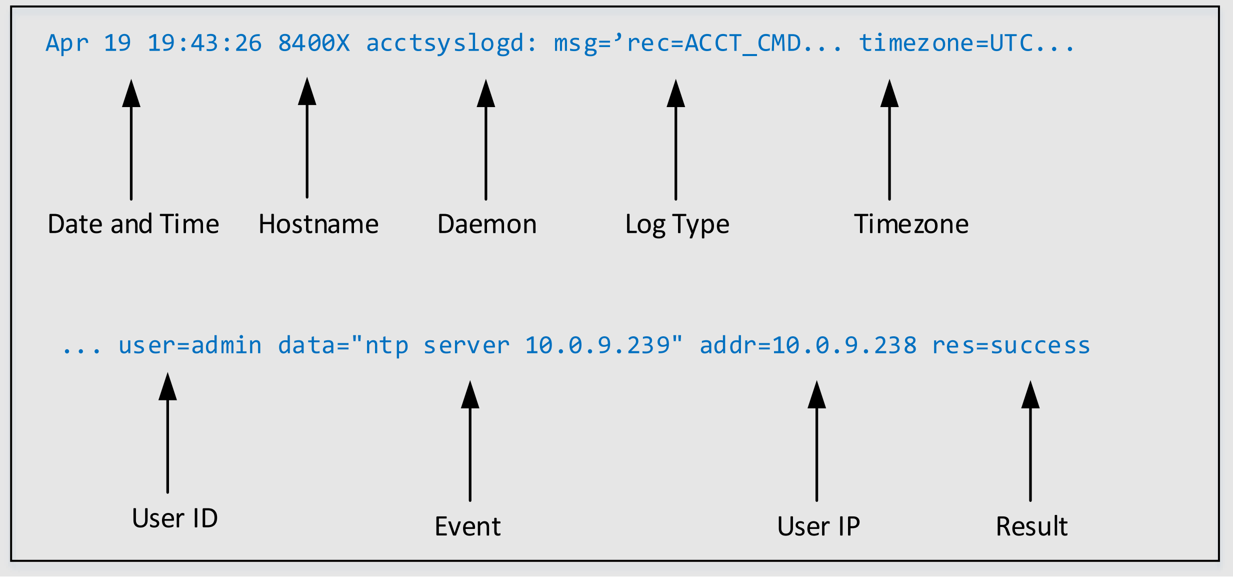
The following table describes each field:

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): **LOG_EMERG** — system is unusable. **LOG_ALERT** — action must be taken immediately. **LOG_CRIT** — critical conditions. **LOG_ERR** — error conditions. **LOG_WARN** — warning conditions. **LOG_NOTICE** — normal but significant conditions. **LOG_INFO** — informational. **LOG_DEBUG** — debug level messages.
Module	The management module role that generated the log entry. AMM indicates active management module, 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 LOG_INFO level):



```
Apr 19 19:43:26 8400X acctsyslogd: msg=’rec=ACCT_CMD... timezone=UTC...
```

```
... user=admin data="ntp server 10.0.9.239" addr=10.0.9.238 res=success
```

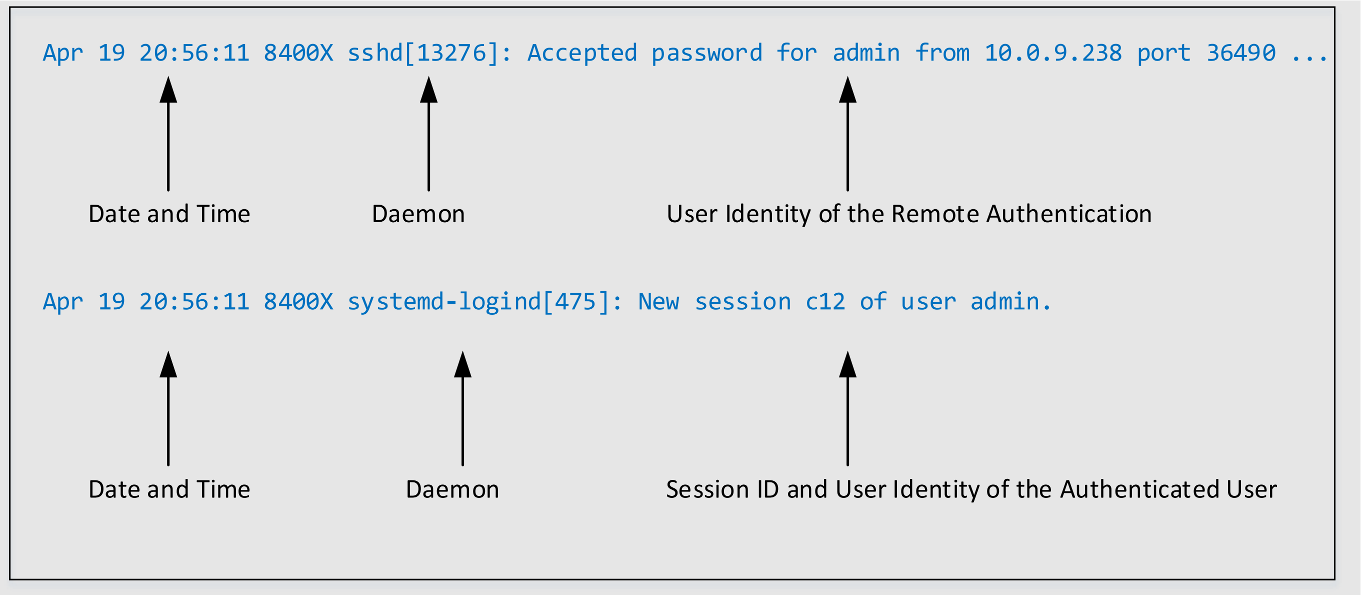
The following table describes each field:

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_EXEC – Login event
Timezone	Timezone of the device.
User ID	The user which 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 authentication log, each log entry includes the following fields (all on 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	Event Message Example
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_ossl:TLS Connection initiated with remote syslog server Disconnection to remote syslog server: 2021-04-29T02:03:25.066462-04:00 HPE8320 rsyslogd - - - nsd_ossl: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 SSH (remote) login failure: 2021-02-28T19:22:01.916264-05:00 HPE8320 sshd[8744] Failed password for admin from 192.168.144.254 port 49660 ssh2 2021-05-07T15:33:12.782396-04:00 HPE8400X sshd 10299 - - Failed publickey for test2 from 192.168.144.253 port 58952 ssh2: RSA May 1 19:34:20 8400X sshd[21904]: Connection closed by authenticating user admin 10.0.9.238 port 32930 [preauth] REST (WebUI) Login: 2023-07-19T15:31:32.985107+00:00 CL-9300 hpe-restd[2487]: Event|4655|LOG_INFO|AMM|-|User gssadmin logged in from 192.168.144.250 through REST session REST (WebUI) Logout: 2023-10-20T13:43:55.656627+00:00 CL-9300 hpe-restd[2505]: Event|4657|LOG_INFO|AMM|-|User gssadmin logged out of REST session from 192.168.144.250 REST (WebUI) login failure: 2023-07-19T15:31:27.198669+00:00 CL-9300 hpe-restd[2487]: Event|4656|LOG_ERR|AMM|-|User gssadmin login from 192.168.144.250 for REST session has failed
	Change to TSF data related to configuration changes	Configuration change by CLI: 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
	Generating/import of changing, or deleting of cryptographic keys	SSH host-key generation: 2021-05-07T15:11:05.276763-04:00 HPE8320 hpe-credmgr 1278 - - Event|6506|LOG_INFO|AMM|1/1|SSH authorized keys were added for user test2.
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	sshd[5005]<190>1 2020-12-07T11:45:33.677860-05:00 HPE8320 sshd 5005 - - Unable to negotiate with 192.168.144.254 port 39364: no matching cipher found. Their offer: aes128-gcm@openssh.com [preauth] sshd[5663]<190>1 2020-12-07T11:55:17.262452-05:00 HPE8320 sshd 5663 - - Unable to negotiate with 192.168.144.254 port 40510: no matching host key type found. Their offer: ssh-rsa [preauth] sshd[6271]<190>1 2020-12-07T12:03:43.811286-05:00 HPE8320 sshd 6271 - - Unable to negotiate with 192.168.144.254 port 41514: no matching MAC found. Their offer: hmac-sha1-96 [preauth] sshd[6479]<190>1 2020-12-07T12:05:56.028125-05:00 HPE8320 sshd 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] 2023-06-01T12:59:50.875471+00:00 myswitch sshd 6701 - - Bad packet length 262156.
FCS_TLSC_EXT.1	Failure to establish a TLS Session	SAN/CN Mismatch IP and Hostname: 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. 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) Cert Validation error: 2021-03-21T22:44:05.883550-04:00 HPE8400X rsyslogd: nsd_ossl:not permitted tolk to peer: certificate validation failed. Status Code : 20 [v8.36.0 try httpwww.rsyslog.com/e/2090] Missing Server Purpose: 2023-08-24T22:50:30.475389+00:00 myswitch rsyslogd - - - nsd_ossl:not permitted to talk to peer: certificate validation

		failed. Status Code : 74 [v8.1908.0 try https://www.rsyslog.com/e/2090] Expired Cert: 2021-03-22T00:27:34.447-04:00 myswitch rsyslogd[4369]: debug|LOG_ERR||The certificate is expired Revoked Cert: 2023-09-05T17:18:13.808035+00:00 myswitch rsyslogd - - - nsd_ossl: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_ossl: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_ossl: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_ossl: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_ossl: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_ossl: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_ossl:not permitted to talk to peer: certificate validation failed. Status Code : 74 [v8.1908.0 try https://www.rsyslog.com/e/2090] No Matching Cipher:

		2023-08-22T23:46:12.206582+00:00 myswitch rsyslogd - - - nsd_ossl:OpenSSL Error Stack: error:140920F8:SSL routines:ssl3_get_server_hello:unknown cipher returned [v8.1908.0] Bad record MAC: 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] Wrong TLS Version: 2023-08-22T23:49:28.253698+00:00 myswitch rsyslogd - - - nsd_ossl:OpenSSL Error Stack: error:1409210A:SSL routines:ssl3_get_server_hello:wrong ssl version [v8.1908.0] Handshake Failure: 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] Wrong certificate type: 2023-08-22T23:45:16.866679+00:00 myswitch rsyslogd - - - nsd_ossl:OpenSSL Error Stack: error:1409017F:SSL routines:ssl3_get_server_certificate:wrong certificate type [v8.1908.0]
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Failed login attempt from SSH or Local console as described by FAU_GEN.1 audit contains the Origin of the Attempt. 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. AND Login Attempt Limit is exceeded: 2021-05-07T16:19:39.868469-04:00 HPE8320 sshd 25938 - - pam_tally2(sshd:auth): user test (1004) tally 6, deny 2
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.	Upon user types in CLI “copy sftp:// … …”: 2020-12-11T11:28:17.539060-05:00 HPE8320 acctsyslogd - - - 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 2020-12-11T11:28:17.536493-05:00 HPE8320 -vtysh 22197 - - 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 2021-01-29T10:40:59.371151-05:00 HPE8320 -vtysh 14571 - - Event|4403|LOG_ERR|AMM|1/1|User admin: secondary image update failed via TFTP from 192.168.144.253
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 update the TOE, and to verify the updates using [digital signature] capability prior to 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 myswitch 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 myswitch 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
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; 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	Upon user types in “clock date 2021-04-26 ”: 2021-04-26T22:53:33.008601-04:00 HPE8320 -vtysh 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

	via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	
FTA_SSL_EXT.1 (if “lock the session” is selected)	Any attempts at unlocking of 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.	Upon user types “exit” from a remote session: 2021-04-28T16:34:44.148667-04:00 HPE6300F sshd 30327 - - Disconnected from user admin 192.168.144.254 port 51250. Upon user types “exit” from a local session: 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. Upon user types “exit” from an HTTPS session: 2023-07-19T17:58:17.248276+00:00 myswitch hpe-restd[2487]: Event|4657|LOG_INFO|AMM|-|User admin logged out of REST session from 192.168.144.250
FTA_TAB.1	None.	
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel.	2021-03-21T22:27:19.698671-04:00 HPE8400X rsyslogd - - - nsd_ossl:TLS Connection initiated with remote syslog server. [v8.36.0] 2021-03-21T22:27:19.755427-04:00 HPE8400X rsyslogd 32000 - - Event|7708|LOG_INFO|UMM|-|Certificate tl34-16x.example.com verified and accepted 2023-08-23T17:51:54.082951+00:00 myswitch rsyslogd - - - nsd_ossl:TLS session terminated with remote syslog server. [v8.1908.0]
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	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 selftest 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.

2 Appendix A: MACsec Configuration

The MACsec functions described in this appendix are provided as support for the evaluation of the model 6300M and 8360 devices. These devices were evaluated against the NDcPP22e and MACsec module. The security claims for this evaluation are outlined in the ***Aruba, a Hewlett Packard Enterprise Company 6300M and 8360 Switch Series MACsec Security Target.*** For all other models, the use of MACsec functionality is not evaluated.

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 myswitch macsecd 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 and 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 configuration of MACsec, please see the section ‘MACsec’ in the AOS-CX 10.13 Security Guide. The instructions below are specific to the configuration for Common Criteria and the evaluated configuration.

MACsec Configuration (using pre-shared keys)

(1) 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
```

To disable or delete a pre-sahred key:`-mka-policy)# no pre-shared-key ckn <key> cak plaintext <key>`

(3) Apply the MACsec and MKA Policy to 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 a 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 ckn <CA-KEY-NAME> cak {plaintext [<PLAINTEXT-CAK>] | ciphertext
<CIPHERTEXT-CAK>}
```

The CKN supports a range of 1 to 64 hexadecimal characters.

MACsec Configuration (using 802.1X EAP TLS)

802.2X EAP TLS is not part of the evaluated configuration and was not tested. It should not be used in an evaluated configuration.

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 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 infinite lifetime:

```
switch(config-keychain-key)# send-lifetime duration infinite
```

Refer 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, configures 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 and indicates that 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 MACsec self tests are run on the TOE, the administrator should enable the self-test with the following command:

```
switch(config)# macsec selftest
```

When enabled, the system will drop traffic on all MACsec capable interfaces until the MACsec selftest completes successfully on the interface. If the self-test fails on one or more interfaces, the administrator must either toggle “macsec selftest“ or reboot the switch to recover the interfaces that failed self-test.

3 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:

HPE Aruba Networking | Enterprise

Once logged in, you can search for documentation related to the product version you are interested in using the “Software and Document search” functionality.

For information regarding changes between 10.13 and the tested 10.11 version, please refer to the 10.13 release notes for the hardware platform you are interested in.

More information is available on the full line of products for Aruba from the following sources:

- Release Notes (Networking Support)
- Aruba website (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